MASARYKOVA UNIVERZITA
PŘÍRODOVĚDECKÁ FAKULTA
ÚSTAV MATEMATIKY A STATISTIKY

Bakalářská práce

BRNO 2015 IVANA BACHUROVÁ

MASARYKOVA UNIVERZITA
PŘÍRODOVĚDECKÁ FAKULTA
ÚSTAV MATEMATIKY A STATISTIKY

Lineární algebra pro pokročilé

Bakalářská práce

Ivana Bachurová

Vedoucí práce: doc. RNDr. Martin Čadek, CSc. **Brno 2015**

Bibliografický záznam

Autor:	Ivana Bachurová Přírodovědecká fakulta, Masarykova univerzita Ústav matematiky a statistiky
Název práce:	Lineární algebra pro pokročilé
Studijní program:	Matematika
Studijní obor:	Finanční a pojistná matematika
Vedoucí práce:	doc. RNDr. Martin Čadek, CSc.
Akademický rok:	2014/2015
Počet stran:	$\mathrm{ix}+41$
Klíčová slova:	Jordanova věta; Jordanův kanonický tvar; endomorfizmus; vlastní číslo; kořenový podprostor; polynom; $\mathbb{T}[x]$-modul; λ-matice; kanonická matice

Bibliografický záznam

Autor:	Ivana Bachurová Prírodovedecká fakulta, Masarykova univerzita Ústav matematiky a štatistiky
Názov práce:	Lineárna algebra pre pokročilých
Študijný program:	Matematika
Študijný odbor:	Finančná a poistná matematika
Vedúci práce:	doc. RNDr. Martin Čadek, CSc.
Akademický rok:	2014/2015
Počet strán:	ix + 41
Kľúčové slová:	Jordanova veta; Jordanov kanonický tvar; endomorfizmus; vlastné číslo; koreňový podpriestor; polynóm; $\mathbb{T}[x]$-modul; $\lambda-$ matica; kanonická matica

Bibliographic Entry

Author:	Ivana Bachurová Faculty of Science, Masaryk University Department of Mathematics and Statistics
Title of Thesis:	Advanced linear algebra
Degree Programme:	Mathematics
Field of Study:	Financial and Insurance Mathematics
Supervisor:	doc. RNDr. Martin Čadek, CSc.
Academic Year:	2014/2015
Number of Pages:	$\mathrm{ix} + 41$
Keywords:	Jordan theorem; Jordan canonical form; endomorfism; eigenvector; root subspace; polynomial; $\mathbb{T}$-modulus; λ-matrix; canonical matrix

Abstrakt

V této práci se věnujeme Jordanově větě a jejím dvěma různým důkazům. V první kapitole nejdříve vyslovíme Jordanovu větu pro endomorfismy a pro matice, a postupně se definováním potřebných pojmů a dokazováním pomocných vět propracujeme ke geometrickému důkazu Jordanovy věty, ve kterém jsou klíčové kořenové podprostory pro vlastní čísla. V druhé kapitole se zabýváme algebraickým důkazem, který se odkazuje na různé algebraické struktury využívající polynomy. Na závěr kapitoly uvedeme algoritmus pro nalezení Jordanova kanonického tvaru, který demonstrujeme na příkladě.

Abstract

This thesis deals with Jordan theorem and two of its different proofs. In the first part, Jordan theorem for endomorphisms and matrices is formulated. Then, by defining necessary terms and proving auxiliary theorems, we provide geometric proof of Jordan theorem, in which root subspaces are crucial. In the second part, we deal with algebraic proof, which refers to various algebraic structures where polynomials are applicable. Then, algorithm for finding Jordan canonical form is shown, which is subsequently demonstrated on an example.

MASARYKOVA UNIVERZITA
Přírodovědecká fakulta

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

Akademický rok: 2014/2015

Ústav: Ústav matematiky a statistiky

Studentka: Ivana Bachurová

Program: Matematika

Obor: Finanční a pojistná matematika

Ředitel *Ústavu matematiky a statistiky* PřF MU Vám ve smyslu Studijního a zkušebního řádu MU určuje bakalářskou práci s tématem:

Téma práce: Lineární algebra pro pokročilé

Téma práce anglicky: Advanced linear algebra

Oficiální zadání:
Cílem práce je prostudovat a zpracovat různé důkazy Jordanovy věty. S tím souvisí studium některých pojmů, které nejsou obsahem základních dvou kurzů lineární algebry na Přírodovědecké fakultě MU. Práce bude psána ve slovenštině.

Literatura:
SLOVÁK, Jan. *Lineární algebra*. Učební texty. Brno: Masarykova univerzita, 1998. 138 s. elektronicky dostupné na www.math.muni.cz/ slovak. ISBN nemá.

BICAN, Ladislav. *Lineární algebra a geometrie*. Vyd. 2. Praha: Academia, 2009. 303 s. ISBN 978-80-200-1707-9.

ZLATOŠ, Pavol. Lineárna algebra a geometria, Bratislava, Albert Marenčin PT, s.r.o., 2011, 741 s. ISBN 978-80-8114-111-9.

Jazyk závěrečné práce: slovenština

Vedoucí práce: doc. RNDr. Martin Čadek, CSc.

Datum zadání práce: 3. 6. 2014

V Brně dne: 29. 10. 2014

Souhlasím se zadáním (podpis, datum):

Bachurová	Čadek	v. z. Paul Hájek
Ivana Bachurová **studentka**	doc. RNDr. Martin Čadek, CSc. **vedoucí práce**	prof. RNDr. Jiří Rosický, DrSc. **ředitel Ústavu matematiky a statistiky**

Poďakovanie

Na tomto mieste by som chcela poďakovať doc. RNDr. Martinovi Čadkovi, CSc. za odbornú pomoc pri vypracovávaní mojej bakalárskej práce, jeho trpezlivosť, ochotu a množstvo času, ktoré venoval konzultáciam k mojej práci a za obohatenie mojich znalostí z lineárnej algebry a geometrie.

Prohlášení

Prohlašuji, že jsem moji bakalářskou práci vypracovala samostatně s využitím informačních zdrojů, které jsou v práci citovány.

Brno 27. května 2015 ....

Ivana Bachurová

Obsah

Úvod

Podobnosť matíc a Jordanova veta o kanonickom tvare patria do základu kurzu lineárnej algebry a geometrie. Študenti matematiky sa tak na začiatku svojho štúdia naučia nielen znenie tejto vety, ale aj jeden z algoritmov hľadania Jordanovho kanonického tvaru. Podrobný dôkaz existencie Jordanovho kanonického tvaru a jeho jednoznačnosti je už náročnejšou témou, na ktorú kvôli jej rozsiahlosti v prednáškach často neostáva čas. V tejto práci sa preto budeme detailne venovať práve dvom rôznym dôkazom Jordanovej vety. Prvý bude využívať skôr geometrické pojmy, budeme sa pohybovať vo vektorových priestoroch a podpriestoroch, kde využijeme znalosti o invariantných podpriestoroch, či reťazcoch vektorov, ktoré sa daným endomorfizmom zobrazujú do seba. Tento prístup ponúka pomerne jednoduchý návod na nájdenie Jordanovho kanonického tvaru pomocou vlastných vektorov a na nich nadväzujúcich reťazcov v jednotlivých koreňových podpriestorov, ktorý je súčasťou kurzu Lineárni algebra a geometrie II na Masarykovej univerzite. Tento spôsob sa však značne komplikuje pri vyšších dimenziách. V druhej kapitole si ukážeme algebraický dôkaz Jordanovej vety, ako aj všeobecne užitočnejší algoritmus pre nájdenie Jordanovho kanonického tvaru, ktorý používa modifikáciu Gaussovej eliminačnej metódy pre matice s polynómami. V literatúre sa častokrát stretávame s rozpracovaním len jednej verzie dôkazu a z neho vyplývajúceho algoritmu. Ako sme už vyššie spomenuli, podrobný dôkaz Jordanovej vety je rozsiahly a časovo náročný, pretože využíva veľké množstvo rôznych pojmov z lineárnej algebry a geometrie. Preto aj v nami používanej literatúre sú niektoré časti iba naznačené. V našej práci sme však súvisiace podrobnosti doplnili. V niektorých úsekoch budú postupy týchto dvoch typov dokazovania rovnaké, všeobecne však využívajú rozličné matematické inštrumenty. Určite je však zaujímavé porovnať tieto zhody a rozdiely, čo bežne učebnice venujúce sa lineárnej algebre a geometrii z vyššie spomenutého dôvodu neponúkajú.

Kapitola 1

Geometrický dôkaz Jordanovej vety

V tejto kapitole si na začiatku pripomenieme základné pojmy súvisiace s témou Jordanovho kanonického tvaru, ktoré poznáme z kurzu lineárnej algebry a geometrie. Prejdeme k formulácii Jordanovej vety a po nej sa budeme zaoberať geometrickým dôkazom, využívajúcom rôzne vlastnosti niektorých typov endomorfizmov. Táto časť čerpá najmä z 5. kapitoly textu Jana Slováka Lineární algebra [4], ale v úvodnej časti si pomôžeme aj 18. a 19. kapitolou knihy Pavla Zlatoša Lineárna algebra a geometria [6].

1.1 Formulácia Jordanovej vety

Na úvod upresnime, že sa budeme pohybovať vo vektorových priestoroch U nad telesom $\mathbb{T}$. Lineárne zobrazenie priestoru U do seba samého sa nazýva endomorfizmus. Symbolicky zapisujeme ako $\varphi : U \to U$. Matica endomorfizmu v danej báze $\alpha = (u_1, u_2, \ldots, u_n)$ je matica tvaru $n \times n$, kde $i-$ty stĺpec tvoria súradnice zobrazeného $i-$teho vektoru bázy α opäť v tejto báze, matematicky zapísané ako

$$(\varphi)_{\alpha,\alpha} = \big((\varphi(u_1))_\alpha, (\varphi(u_2))_\alpha, \ldots, (\varphi(u_n))_\alpha\big).$$

Veľmi dôležitou súčasťou témy Jordanovho kanonického tvaru, budeme tiež používať skratku JKT, sú vlastné čísla, prípadne označované aj ako vlastné alebo charakteristické hodnoty. Vlastné číslo endomorfizmu φ je skalár λ, pre ktorý platí, že vo vektorovom priestore U existuje nenulový vektor u taký, že

$$\varphi(u) = \lambda u.$$

Tento vektor nazývame vlastný vektor endomorfizmu φ prislúchajúci vlastnej hodnote λ. Množinu všetkých vlastných čísel endomorfizmu φ označujeme pojmom spektrum endomorfizmu. Vlastný podpriestor príslušný vlastnému číslu λ je podpriestor v U definovaný ako jadro endomorfizmu $\varphi - \lambda \mathrm{id}$. Determinant matice $\mathbf{A} - \lambda\mathbf{E}$, kde matica $\mathbf{A}$ je maticou endomorfizmu φ v nejakej báze, definujeme ako charakterictický polynóm endomorfizmu φ. Maticu $\mathbf{A} - \lambda\mathbf{E}$ označujeme pojmom charakteristická matica matice $\mathbf{A}$. Charakterický polynóm je určený jednoznačne, čiže nezávisí od výberu bázy a množina jeho koreňov je rovná spektru endomorfizmu φ. Násobnosť koreňa λ charakterického polynómu označujeme pojmom algebraická násobnosť vlastného čísla λ. Dimenziu jadra endomorfizmu

$\varphi - \lambda\mathrm{id}$ definujeme zas ako geometrickú násobnosť. Pripomeňme tiež pojem podobnosti matíc. Dve matice $\mathbf{A}$ a $\mathbf{B}$ nazveme podobnými, ak existuje invertibilná matica $\mathbf{P}$ taká, že platí $\mathbf{A} = \mathbf{P}^{-1}\,\mathbf{B}\,\mathbf{P}$. Nech α a β sú dve rôzne bázy priestoru U. Potom matica endomorfizmu $\mathbf{A} = (\varphi)_{\alpha,\alpha}$ bude podobná matici $\mathbf{B} = (\varphi)_{\beta,\beta}$, kde $\mathbf{P} = (\mathrm{id})_{\beta,\alpha}$ je maticou prechodu.

Definícia 1.1. Maticu $\mathbf{J}_k(\lambda)$ v tvare

$$\mathbf{J}_k(\lambda) = \begin{pmatrix} \lambda & 1 & 0 & \dots & 0 \\ 0 & \lambda & 1 & \dots & 0 \\ 0 & 0 & \lambda & \dots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \dots & \lambda \end{pmatrix}$$

nazývame Jordanova bunka rádu k príslušná vlastnému číslu λ. O matici $\mathbf{J}$ hovoríme, že je v Jordanovom kanonickom tvare, pokiaľ je blokovo diagonálna s Jordanovymi bunkami na diagonále.

Veta 1.2 (Jordanova veta pre endomorfizmy)**.** *Nech endomorfizmus $\varphi : U \to U$ má súčet algebraických násobností vlastných čísel rovný dimenzii U. Potom existuje taká báza α priestoru U, v ktorej bude mať endomorfizmus φ maticu v Jordanovom kanonickom tvare. Táto matica je až na poradie buniek určená jednoznačne.*

Veta 1.3 (Jordanova veta pre matice)**.** *Nech charakteristický polynóm matice $\mathbf{A}$ tvaru $n \times n$ má vrátane násobností n koreňov. Potom existuje invertibilná matica $\mathbf{P}$ taká, že matica $\mathbf{J} = \mathbf{P}^{-1}\mathbf{A}\mathbf{P}$ je v Jordanovom kanonickom tvare. Táto matica je až na poradie buniek určená jednoznačne.*

Tieto dve vyjadrenia Jordanovej vety sú ekvivalentné.

Dôkaz. Ekvivalenciu medzi vlastnými číslami endomorfizmu a koreňmi charakteristického polynómu sme spomenuli v úvode tejto podkapitoly. Podrobný dôkaz možno nájsť pri vete 18.3.1. v [6].
Jordanova veta pre endomorfizmy implikuje Jordanovu vetu pre matice: Nech $\mathbf{A}$ je matica $n \times n$ taká, že súčet algebraických násobností koreňov charakteristického polynómu je n. Uvažujme $\varphi : \mathbb{T}^n \to \mathbb{T}^n$ definované v štandardnej báze ε predpisom $\varphi(x) = \mathbf{A}x$. Teda $(\varphi)_{\varepsilon,\varepsilon} = \mathbf{A}$. Podľa Jordanovej vety pre endomorfizmy existuje báza α taká, že $(\varphi)_{\alpha,\alpha} = \mathbf{J}$ je matica v JKT. Teda

$$(\varphi)_{\alpha,\alpha} = (\mathrm{id})_{\alpha,\varepsilon}(\varphi)_{\varepsilon,\varepsilon}(\mathrm{id})_{\varepsilon,\alpha}$$

a preto

$$\mathbf{J} = \mathbf{P}^{-1}\mathbf{A}\mathbf{P}.$$

Vidíme, že $\mathbf{A}$ je podobná matici $\mathbf{J}$ v Jordanovom kanonickom tvare.
Jordanova veta pre matice implikuje Jordanovu vetu pre endomorfizmy: Majme $\varphi : U \to U$ a vezmime nejakú jeho bázu $\beta = (u_1, u_2, \dots, u_n)$. Potom $(\varphi)_{\beta,\beta} = \mathbf{A}$ je matica, ktorá splňuje predpoklady Jordanovej vety pre matice. Teda existuje matica $\mathbf{J}$ v JKT taká, že

$$\mathbf{J} = \mathbf{P}^{-1}\mathbf{A}\mathbf{P}.$$

Uvážme bázu $\alpha = (v_1, v_2, \dots, v_n) = (u_1, u_2, \dots, u_n)\mathbf{P}$. V tejto báze je

$$\begin{aligned}(\varphi)_{\alpha,\alpha} &= (\mathrm{id})_{\alpha,\beta}(\varphi)_{\beta,\beta}(\mathrm{id})_{\beta,\alpha}\\ &= \mathbf{P}^{-1}(\varphi)_{\beta,\beta}\mathbf{P}\\ &= \mathbf{P}^{-1}\mathbf{A}\mathbf{P} = \mathbf{J}.\end{aligned}$$

□

1.2 Koreňové podpriestory

V tejto časti si zadefinujeme pojem koreňových podpriestorov. Tieto podpriestory sú rozšírením vlastných podpriestorov a viažu sa vždy k jednému vlastnému číslu. Ešte pripomeňme pojem invariantného podpriestoru endomorfizmu $\varphi : U \to U$, ktorý označuje podpriestor v U, ktorý sa prostredníctvom φ zobrazuje sám do seba.

Definícia 1.4. Majme vektorový priestor U a na ňom endomorfizmus $\varphi\colon U \to U$. Nech λ je vlastným číslom endomorfizmu φ. Potom podpriestor

$$\mathscr{R}_\lambda = \{u \in U;\ \exists j \in \mathbb{N}:\ (\varphi - \lambda\mathrm{id})^j(u) = 0\}$$

nazveme koreňovým podpriestorom vlasného čísla λ.

Nech $\mathscr{R}_\lambda$ má bázu $(u_1, u_2, \dots, u_k)$, kde $u_s \in \mathrm{Ker}(\varphi - \lambda\mathrm{id})^{j_s}$. Označme $m =$ $= \max(j_1, j_2, \dots, j_k)$. Potom

$$\mathscr{R} = \bigcup_{j=1}^{\infty} \mathrm{Ker}(\varphi - \lambda\mathrm{id})^j = \bigcup_{j=1}^{m} \mathrm{Ker}(\varphi - \lambda\mathrm{id})^j = \mathrm{Ker}(\varphi - \lambda\mathrm{id})^m,$$

pretože každé $u \in \mathscr{R}_\lambda$ je tvaru $u = \sum_{s=1}^{k} a_s u_s$ a preto

$$(\varphi - \lambda\mathrm{id})^m(u) = (\varphi - \lambda\mathrm{id})^m(\sum_{s=1}^{k} a_s u_s) = \sum_{s=1}^{k} a_s(\varphi - \lambda\mathrm{id})^m(u_s) = 0.$$

Lema 1.5. *Majme endomorfizmy φ a ψ. Nech platí*

$$\varphi \circ \psi = \psi \circ \varphi,$$

potom Ker φ *je invariantný podpriestor pre endomorfizmus ψ.*

Dôkaz. Nech $v \in \mathrm{Ker}\,\varphi$, potom $\varphi(\psi(v)) = \psi(\varphi(v)) = \psi(0) = 0$ a teda $\psi(v) \in \mathrm{Ker}\,\varphi$. □

Predchádzajúcu lemu aplikujeme na endomorfizmy $(\varphi - \lambda\mathrm{id})$ a $(\varphi - \mu\mathrm{id})$, kde $\mu \in \mathbb{T}$. Tým dokážeme, že lema platí aj pre dvojicu endomorfizmov $(\varphi - \lambda\mathrm{id})^m$ a $(\varphi - \mu\mathrm{id})$.

$$\begin{aligned}(\varphi - \lambda\mathrm{id}) \circ (\varphi - \mu\mathrm{id}) &= (\varphi \circ \varphi - \lambda\mathrm{id} \circ \varphi - \varphi \circ \mu\mathrm{id} + \lambda\mathrm{id} \circ \mu\mathrm{id})\\ &= (\varphi \circ \varphi - \varphi \circ \lambda\mathrm{id} - \mu\mathrm{id} \circ \varphi + \mu\mathrm{id} \circ \lambda\mathrm{id})\\ &= (\varphi - \mu\mathrm{id}) \circ (\varphi - \lambda\mathrm{id})\end{aligned}$$

Vidíme, že $\mathscr{R}_\lambda$ je invariantný pre endomorfizmus $(\varphi - \mu\mathrm{id})$ a teda aj pre endomorfizmus φ.

1.3 Direktný súčet podpriestorov

Pripomenieme si pojem direktného súčtu podpriestorov a niektoré jeho vlastnosti.

Definícia 1.6. Súčet podpriestorov $U_1, U_2, \ldots, U_k \subseteq U$ je podprietor

$$U_1 + U_2 + \ldots + U_k = \{u_1 + u_2 + \ldots u_k \in U, \text{ kde } u_i \in U_i\}.$$

Definícia 1.7. Súčet podpriestorov $U_1, U_2, \ldots, U_k \subseteq U$ je direktným súčtom, ak pre každé $u \in U_1 + U_2 + \ldots + U_k$ existuje práve jedna k-tica $(u_1, u_2, \ldots, u_k) \in U_1 \times U_2 \times \ldots \times U_k$ tak, že

$$u = u_1 + u_2 + \ldots + u_k.$$

Direktný súčet značíme nasledovne

$$U_1 \oplus U_2 \oplus \ldots \oplus U_k.$$

Lema 1.8. *Súčet podpriestorov $U_1 + U_2 + \ldots + U_k$ je direktný, práve keď pre všetky k-tice $u_1, u_2, \ldots, u_k \in U_1 \times U_2 \times \ldots \times U_k$ rovnosť*

$$u_1 + u_2 + \ldots + u_k = 0$$

implikuje

$$u_1 = u_2 = \ldots = u_k = 0.$$

Dôkaz. Nech $U_1 + U_2 + \ldots + U_k$ je direktný a nech $u_1 + u_2 + \ldots + u_k = 0$. Pretože $0 \in U_1 + U_2 + \ldots + U_k$ a môžme ju rozpísať ako

$$0 + 0 + \ldots + 0 = 0,$$

tak z jednoznačnosti plynie

$$u_1 = 0, u_2 = 0, \ldots, u_k = 0.$$

Ostáva dokázať opačnú implikáciu. Nech

$$u = u_1 + u_2 + \ldots + u_k \quad u_i \in U_i$$

$$u = v_1 + v_2 + \ldots + v_k \quad v_i \in U_i.$$

Potom odčítaním dostaneme

$$(u_1 - v_1) + (u_2 - v_2) + \ldots + (u_k - v_k) = 0.$$

Odtiaľ

$$u_1 - v_1 = u_2 - v_2 = \ldots = u_k - v_k = 0,$$

a preto

$$u_1 = v_1, u_2 = v_2, \ldots, u_k = v_k.$$

Z toho plynie jednoznačnosť definujúca direktný súčet. □

Lema 1.9. *Nech $U_1, U_2 \dots, U_n$ sú podpriestory v U. Nasledujúce podmienky sú ekvivalentné*

1. *súčet podpriestorov $U_1, U_2 \dots, U_n$ je direktný*
2. $U_i \cap (U_1 + \dots + U_{i-1} + U_{i+1} + \dots + U_n) = 0 \qquad$ *pre* $1 \leq i \leq n$.

Dôkaz. (1) implikuje (2) dokážeme obmenou implikácie. Uvažujme nenulový vektor $u \in U_i \cap (U_1 + \dots + U_{i-1} + U_{i+1} + \dots + U_n)$, kde $1 \leq i \leq n$. Potom môžme u napísať dvoma spôsobmi ako

$$\begin{aligned} u &= u_i \\ u &= u_1 + \dots + u_{i-1} + u_{i+1} + \dots + u_k, \end{aligned}$$

pre nejaké $u_1 \in U_1, u_2 \in U_2, \dots, u_n \in U_n$. Odtiaľ odčítaním dostávame

$$u_1 + \dots + u_{i-1} - u_i + u_{i+1} + \dots + u_n = 0,$$

a teda podľa predchádzajúcej lemy 1.8

$$u_1 = \dots = u_{i-1} = -u_i = u_{i+1} = \dots = u_n = 0.$$

To je ale spor s predpokladom, že $u \neq 0$.
(2) implikuje (1) dokážeme takisto obmenou implikácie. Ak súčet nie je direktný, tak podľa lemy 1.8 môžme vektor 0 napísať ako

$$0 = u_1 + u_2 + \dots + u_n$$

pre nejaké $u_i \neq 0$. Potom

$$-u_i = u_1 + u_2 + \dots + u_{i-1} + u_{i+1} + \dots + u_n.$$

Z tejto rovnice vidíme, že nenulový vektor $-u_i$ leží aj v U_i, aj v súčte podpriestorov $U_1 + \dots + U_{i-1} + U_{i+1} + \dots + U_n$, čiže sme dokázali, že keď neplatí tvrdenie (1), neplatí ani tvrdenie (2). □

1.4 Definícia a vlastnosti kvocientu

V tejto podkapitole si najskôr definujeme pojem kvocient a odvodíme niektoré jeho vlastnosti, ktoré budú pre nás dôležité. Prejdeme k definíciam polorozpadnutej a rozpadnutej matice, a ukážeme súvislosti medzi kvocientom s invariantným podpriestorom V a maticou endomorfizmu φ v polorozpadnutom stave. Všimnime si, že tieto poznatky nás postupne približujú k blokovo diagonálnemu tvaru matice endomorfizmu, čo je jedným z našich cieľov.

Definícia 1.10. Nech V je vektorový podpriestor v U. Pre $u \in U$ definujeme množinu

$$u + V = \{(u + v) \in U, v \in V\}.$$

Lema 1.11. *Nech $u_1, u_2 \in U$. Potom rovnosť*

$$u_1 + V = u_2 + V$$

platí práve vtedy, keď $u_1 - u_2 \in V$.

Dôkaz. Rovnosť $u_1 + V = u_2 + V$ znamená, že pre každé $v_1 \in V$ existuje $v_2 \in V$ také, že

$$u_1 + v_1 = u_2 + v_2.$$

Odtiaľ

$$u_1 - u_2 = v_2 - v_1 \in V.$$

Naopak pokiaľ $u_1 - u_2 \in V$, potom pre každé $v \in V$ je

$$u_1 + v = u_2 + (u_1 - u_2 + v),$$

kde $u_1 - u_2 + v \in V$ a odtiaľ vidíme, že $u_1 + V \subseteq u_2 + V$.
Analogicky dokážeme $u_2 + V \subseteq u_1 + V$. □

Definícia 1.12. Kvocient

$$U/V = \{u + V, u \in U\}$$

s operáciami sčítania

$$(u_1 + V) + (u_2 + V) = (u_1 + u_2) + V$$

a násobenia

$$c(u + V) = (cu) + V$$

je vektorový priestor.

Najprv ukážeme, že definícia súčtu a násobku je korektná.
Chceme dokázať, že keď

$$\begin{aligned} u_1 + V &= \overline{u_1} + V \\ u_2 + V &= \overline{u_2} + V, \end{aligned}$$

potom

$$(u_1 + u_2) + V = (\overline{u_1} + \overline{u_2}) + V$$

$$cu_1 + V = c\overline{u_1} + V.$$

V prvom prípade nastane rovnosť podľa lemy 1.11 práve vtedy, keď $(u_1 + u_2) - (\overline{u_1} + \overline{u_2}) \in V$.

$$(u_1 + u_2) - (\overline{u_1} + \overline{u_2}) = (u_1 - \overline{u_1}) + (u_2 - \overline{u_2}),$$

kde $u_1 - \overline{u_1} \in V$ a $u_2 - \overline{u_2} \in V$, čo vyplýva z predpokladu a teda aj ich súčet leží vo V.
V druhej rovnici rovnako použijeme lemu 1.11, podľa ktorej rovnosť platí, ak $cu_1 - c\overline{u_1} \in V$.

$$cu_1 - c\overline{u_1} = c(u_1 - \overline{u_1}),$$

kde $u_1 - \overline{u_1} \in V$ podľa predpokladu, čiže aj $c(u_1 - \overline{u_1}) \in V$.
Vlastnosti sčítania a násobenia na U/V plynú z vlastností sčítania a násobenia na U.
Definícia je korektná. $(U/V, +, \cdot)$ je vektorový priestor.

Definícia 1.13. Maticu tvaru

$$\begin{pmatrix} \mathbf{A} & 0 \\ 0 & \mathbf{B} \end{pmatrix},$$

kde $\mathbf{A}$ a $\mathbf{B}$ sú nejaké nenulové matice nazveme rozpadnutou maticou. Maticu tvaru

$$\begin{pmatrix} \mathbf{A} & \mathbf{C} \\ 0 & \mathbf{B} \end{pmatrix},$$

kde $\mathbf{A}$, $\mathbf{B}$ a $\mathbf{C}$ sú nejaké nenulové matice nazveme polorozpadnutou maticou.

Veta 1.14. *Majme priestor U a endomorfizmus $\varphi : U \to U$. Nech U je direktným súčtom dvoch invariantných podpriestorov: $U = U_1 \oplus U_2$. Potom existuje v U báza $\alpha = (u_1, u_2, \dots, u_n)$, v ktorej je matica endomorfizmu φ rozpadnutá.*

Dôkaz. Nech $\alpha' = (u_1, u_2, \dots, u_k)$ je bázou invariantného podpriestoru U_1
a $\alpha'' = (u_{k+1}, u_{k+2}, \dots, u_n)$ je bázou invariantného podpriestoru U_2. Maticu endomorfizmu φ v báze $\alpha = (u_1, \dots, u_k, u_{k+1}, \dots, u_n)$ píšme v tvare

$$(\varphi)_{\alpha,\alpha} = \begin{pmatrix} \mathbf{A} & \mathbf{C} \\ \mathbf{D} & \mathbf{B} \end{pmatrix},$$

kde $\mathbf{A}$ je tvaru $k \times k$, $\mathbf{C}$ je tvaru $k \times (n-k)$, $\mathbf{D}$ je tvaru $(n-k) \times k$ a nakoniec $\mathbf{B}$ je tvaru $(n-k) \times (n-k)$. Vektory z bázy α' zobrazíme takto:

$$\varphi(u_i) = a_{1i}u_1 + a_{2i}u_2 + \ldots + a_{ki}u_k + d_{k+1i}u_{k+1} + \ldots + d_{ni}u_n$$

pre $1 \leq i \leq k$. Keďže vieme, že podpriestor U_1 je invariantný, tak koeficienty $i-$teho stĺpca matice $\mathbf{D}$ budú nulové pre všetky i. Rovnako postupujeme aj pre bázové vektory invariantného podpriestoru U_2, kde vo vzťahu

$$\varphi(u_i) = c_{1i}u_1 + c_{2i}u_2 + \ldots + c_{ki}u_k + b_{k+1i}u_{k+1} + \ldots + b_{ni}u_n$$

pre $k+1 \leq i \leq n$ budú koeficienty matice $\mathbf{C}$ nulové, keďže stoja pri vektoroch, ktoré neležia v U_2. □

Veta 1.15. *Nech $\varphi : U \to U$ je endomorfizmus a $V \subset U$ invariantný podpriestor. Predpokladajme, že báza $\alpha = (u_1, u_2, \dots, u_n)$ priestoru U vznikla rozšírením bázy $(u_1, u_2, \dots, u_k)$ podpriestoru V. Definujme endomorfizmus $\widetilde{\varphi} : U/V \to U/V$ nasledovným spôsobom*

$$\widetilde{\varphi}(u+V) = \varphi(u) + V.$$

Potom

$$(\varphi)_{\alpha,\alpha} = \begin{pmatrix} \mathbf{A} & \mathbf{C} \\ 0 & \mathbf{B} \end{pmatrix}.$$

Navyše platí, že $\widetilde{\alpha} = (u_{k+1} + V, \dots, u_n + V)$ je bázou U/V a $(\widetilde{\varphi})_{\widetilde{\alpha},\widetilde{\alpha}} = B$.

Dôkaz. Najprv overíme korektnosť definície endomorfizmu $\widetilde{\varphi}(u+V)=\varphi(u)+V$. Nech $u+V=\overline{u}+V$. Potom $u-\overline{u}\in V$. Z invariantnosti podpriestoru V plynie, že

$$\varphi(u)-\varphi(\overline{u})=\varphi(u-\overline{u})\in V$$

a teda

$$\varphi(u)+V=\varphi(\overline{u})+V.$$

Tvrdenie o polorozpadnutom tvare matice $(\varphi)_{\alpha,\alpha}$ sa dokáže podobne ako predchádzajúca veta 1.14. Keďže podpriestor V dimenzie k je invariantný, tak sa prvých k vektorov bázy α zobrazí opäť do podpriestoru V. To vysvetluje nulovú maticu tvaru $(n-k)\times k$ pod maticou $\mathbf{A}$, pričom matica $\mathbf{A}$ je maticou endomorfizmu z $V\to V$.

Ďalej dokážeme tvrdenie o báze vektorového podpriestoru U/V. Vektor $u\in U$ môžme rozpísať ako lineárnu kombináciu vektorov bázy U :

$$u=\sum_{i=1}^{n}a_iu_i.$$

Potom môžme rozpísať aj vektor $u+V\in U/V$:

$$u+V=\sum_{i=1}^{n}a_iu_i+V=\left(\sum_{i=1}^{k}a_iu_i+\sum_{i=k+1}^{n}a_iu_i\right)+V=\sum_{i=k+1}^{n}a_iu_i+V=\sum_{i=k+1}^{n}a_i(u_i+V)$$

podľa lemy 1.11. Vidíme, že prvky $u_{k+1}+V,u_{k+2}+V,\dots,u_n+V$ generujú podpriestor U/V.
Ostáva dokázať, že všetky tieto prvky sú lineárne nezávislé v U/V. Nech

$$\sum_{i=k+1}^{n}a_i(u_i+V)=0+V.$$

Potom

$$\sum_{i=k+1}^{n}a_iu_i+V=0+V,$$

$$\sum_{i=k+1}^{n}a_iu_i-0\in V,$$

$$\sum_{i=k+1}^{n}a_iu_i=\sum_{i=1}^{k}a_iu_i$$

pre nejaké $a_1,a_2,\dots,a_k\in\mathbb{K}$ a teda

$$-a_1u_1-a_2u_2+\dots-a_ku_k+a_{k+1}u_{k+1}+\dots+a_nu_n=0.$$

Vieme, že $u_1,\dots,u_n$ sú lineárne nezávislé a preto

$$a_1=\dots=a_k=a_{k+1}=\dots=a_n=0.$$

Posledné tvrdenie, ktoré treba dokázať, je o tvare matice endomorfizmu $(\widetilde{\varphi})_{\widetilde{\alpha},\widetilde{\alpha}}$. Už sme ukázali, že matica $(\varphi)_{\alpha,\alpha}$ má tvar $\left(\begin{smallmatrix} A & C \\ 0 & B \end{smallmatrix}\right)$. Matice **C** a **B** si pre lepšiu predstavu rozpíšeme.

$$\mathbf{C} = \begin{pmatrix} c_{11} & c_{12} & \dots & c_{1n-k} \\ c_{21} & c_{22} & \dots & c_{2n-k} \\ \vdots & \vdots & \ddots & \vdots \\ c_{k1} & c_{k2} & \dots & c_{kn-k} \end{pmatrix} \qquad \mathbf{B} = \begin{pmatrix} b_{11} & b_{12} & \dots & b_{1n-k} \\ b_{21} & b_{22} & \dots & b_{2n-k} \\ \vdots & \vdots & \ddots & \vdots \\ b_{n-k1} & b_{n-k2} & \dots & b_{n-kn-k} \end{pmatrix}$$

Maticu $(\widetilde{\varphi})_{\widetilde{\alpha},\widetilde{\alpha}}$ spočítame podľa definície. Pre $1 \leq i \leq n-k$ je

$$\begin{aligned} \widetilde{\varphi}(u_{k+i}+V) = \varphi(u_{k+i}) + V & \\ &= c_{1i}u_1 + \ldots + c_{ki}u_k + b_{1i}u_{k+1} + \ldots + b_{n-ki}u_n + V \\ &= b_{1i}(u_{k+1}+V) + \ldots + b_{n-ki}(u_n+V). \end{aligned}$$

Koeficienty z matice **C** prispievajú len do podpriestoru V a preto matica endomorfizmu v indukovanej báze $\widetilde{\alpha}$ zodpovedá matici **B**. □

Lema 1.16. *Nech U je vektorový priestor s bázou $(u_1, u_2, \ldots, u_n)$, ktorá je rozšírením bázy $(u_1, u_2, \ldots, u_k)$ podpriestoru V. Potom*

$$\dim U/V = \dim U - \dim V.$$

Dôkaz. Nech $\dim U = n$ a $\dim V = k$. Podľa vety 1.15 má podpriestor U/V bázu $\widetilde{\alpha} = (u_{k+1}+V, u_{k+2}+V, \ldots, u_n+V)$ a rovno vidíme, že túto bázu tvorí $n-k$ prvkov. □

1.5 Rozklad priestoru na direktný súčet koreňových podpriestorov

Predchádzajúce podkapitoly sa venovali niektorým všeobecným nástrojom lineárnej algebry a geometrie. V nasledujúcej časti ich konečne využijeme a ukážeme prvý dôležitý krok k dôkazu Jordanovej vety. Doteraz nadobudnuté znalosti nám umožnia rozložiť vektorový priestor U na direktný súčet koreňových podpriestorov, o ktorých vieme, že sú invariantné vzhľadom k endomorfizmu φ, čo v praxi znamená, že existuje báza tohto priestoru, v ktorej nadobudne matica endomorfizmu φ blokovo diagonálny tvar, pričom jednotlivé bloky budú určené vlastnými číslami a ich algebraickou násobnosťou. To nám však požadovaný Jordanov kanonický tvar neprinesie a preto spôsob hľadania tejto bázy podriadime ešte podrobnejšiemu rozkladu jednotlivých koreňových podpriestorov, čomu sa ale bude venovať ďalšia časť tejto práce.

Veta 1.17. *Majme endomorfizmus $\varphi : U \to U$ taký, že súčet algebraických násobností jeho vlastných čísel je $\dim U = n$. Potom v U existuje báza α, pre ktorú platí, že*

$$(\varphi)_{\alpha,\alpha} = \begin{pmatrix} \lambda_1 & * & * & \dots & * \\ 0 & \lambda_{i_2} & * & \dots & * \\ 0 & 0 & \lambda_{i_3} & \dots & * \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \dots & \lambda_k \end{pmatrix}$$

Dôkaz. Dôkaz urobíme indukciou podľa $\dim U = n$. Pre $\dim U = 1$ veta zjavne platí. Nech platí pre $\dim U = n-1$. Vektor u_1 nech je vlastným vektorom k vlastnému číslu λ_1 a nech $\alpha = (u_1, u_2, \ldots, u_n)$ je báza priestoru U. Položme $V = [u_1]$. Potom ako sme dokázali vo vete 1.15 je $\widetilde{\alpha} = (u_2 + V, u_3 + V, \ldots, u_n + V)$ bázou priestoru U/V. Endomorfizmus $\widetilde{\varphi} : U/V \to U/V$, kde $V \subset U$ je invariantný podpriestor vzhľadom k endomorfizmu $\varphi : U \to U$ sme si definovali v predchádzajúcej časti nasledovným spôsobom

$$\widetilde{\varphi}(u+V) = \varphi(u) + V.$$

Charakteristický polynóm $\varphi : U \to U$ je

$$\det((\varphi)_{\alpha,\alpha} - \lambda E) = (\lambda_1 - \lambda)^{j_1} \cdot (\lambda_2 - \lambda)^{j_2} \cdot \ldots \cdot (\lambda_k - \lambda)^{j_s},$$

kde $j_1 + \ldots + j_s = n$. Matica endomorfizmu v báze α má podľa vety 1.15 tvar

$$(\varphi)_{\alpha,\alpha} = \begin{pmatrix} \lambda_1 & a_{12} & \cdots & a_{1n} \\ 0 & a_{22} & & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ 0 & a_{n2} & \cdots & a_{nn} \end{pmatrix}$$

pritom matica endomorfizmu $(\widetilde{\varphi})_{\widetilde{\alpha},\widetilde{\alpha}} : U/V \to U/V$ je

$$(\widetilde{\varphi})_{\widetilde{\alpha},\widetilde{\alpha}} = \begin{pmatrix} a_{22} & \cdots & a_{2n} \\ \vdots & \ddots & \vdots \\ a_{n2} & \cdots & a_{nn} \end{pmatrix}.$$

Charakteristický polynóm matice endomorfizmu $(\varphi)_{\alpha,\alpha}$ môžme rozpísať ako

$$\begin{aligned} \det\big((\varphi)_{\alpha,\alpha} - \lambda \mathbb{E}_n\big) &= (\lambda_1 - \lambda) \det\big((\widetilde{\varphi}_{\widetilde{\alpha},\widetilde{\alpha}}) - \lambda \mathbb{E}_{n-1}\big) \\ &= (\lambda_1 - \lambda)^{j_1} \cdot \ldots \cdot (\lambda_k - \lambda)^{j_s} \\ &= (\lambda_1 - \lambda)(\lambda_1 - \lambda)^{j_1 - 1} \cdot \ldots \cdot (\lambda_k - \lambda)^{j_s}, \end{aligned}$$

kde $j_1 + \ldots + j_s = n$. Vidíme, že $j_1 - 1 + \ldots + j_s = n - 1$ a teda endomorfizmus $\widetilde{\varphi} : U/V \to U/V$, kde $\dim U/V = n-1$, splňuje predpoklady vety a teda podľa indukčného predpokladu existuje báza $\widetilde{\beta}$ v U/V taká, že

$$(\widetilde{\varphi})_{\widetilde{\beta},\widetilde{\beta}} = \begin{pmatrix} \lambda_{i_2} & * & \cdots & * \\ 0 & \lambda_{i_3} & & * \\ \vdots & & \ddots & \vdots \\ 0 & & \cdots & \lambda_k \end{pmatrix}$$

$\widetilde{\beta} = (v_2 + V, v_3 + V, \ldots, v_n + V)$.
Vezmeme bázu $\beta = (u_1, v_2, \ldots, v_n)$ a v nej maticu endomorfizmu

$$(\varphi)_{\beta,\beta} = \left(\begin{array}{c|c} \lambda_1 & * \\ \hline & \\ & (\widetilde{\varphi}_{\widetilde{\beta},\widetilde{\beta}}) \\ & \end{array}\right) = \begin{pmatrix} \lambda_1 & * & * & \cdots & * \\ 0 & \lambda_{i_2} & * & & * \\ 0 & 0 & \lambda_{i_3} & & * \\ \vdots & & & \ddots & \vdots \\ 0 & & \cdots & & \lambda_k \end{pmatrix}.$$

□

Veta 1.18. *Majme vektorový priestor U a endomorfizmus $\varphi : U \to U$. Nech súčet algebraických násobností jeho vlastných čísel je $\dim U = n$. Potom platí*

$$U = \mathscr{R}_{\lambda_1} \oplus \mathscr{R}_{\lambda_2} \oplus \ldots \oplus \mathscr{R}_{\lambda_k},$$

kde $\lambda_1, \ldots, \lambda_k$ sú všetky vlastné čísla. Navyše pre všetky vlastné čísla platí, že vektorový podpriestor $\mathscr{R}_{\lambda_)}$ má dimenziu rovnú algebraickej násobnosti príslušného vlastného čísla.

Dôkaz. Dôkaz urobíme postupne. Najprv indukciou podľa počtu sčítancov dokážeme, že súčet je direktný. Predpokladajme, že veta platí pre $k-1$ sčítancov. Majme vektory $u_i \in \mathscr{R}_{\lambda_i}$ také, že $u_1 + u_2 + \ldots + u_k = 0$. Zvoľme m také, že

$$(\varphi - \lambda_k \mathrm{id})^m (u_k) = 0$$

a položme

$$y_i = (\varphi - \lambda_k \mathrm{id})^m (u_i) \qquad \text{pre } 1 \leq i \leq k.$$

Pre y_k platí, že

$$y_k = (\varphi - \lambda_k \mathrm{id})^m (u_k) = 0.$$

Preto

$$\sum_{i=1}^{k-1} y_i = \sum_{i=1}^{k} (\varphi - \lambda_k \mathrm{id})^m (u_i) = (\varphi - \lambda_k \mathrm{id})^m \left(\sum_{i=1}^{k} u_i \right) = 0.$$

Podľa lemy 1.5 ležia vektory y_i pre $1 \leq i \leq k-1$ opäť v príslušných koreňových podpriestoroch a teda podľa indukčného predpokladu a lemy 1.8

$$y_1 = y_2 = \ldots = y_{k-1} = 0.$$

Dokážeme, že endomorfizmus $\varphi - \lambda_k \mathrm{id} : \mathscr{R}_{\lambda_i} \to \mathscr{R}_{\lambda_i}$ je izomorfizmus pre $i = 1, 2, \ldots, k-1$. Potom je izomorfizmom aj endomorfizmus $(\varphi - \lambda_k \mathrm{id})^m : \mathscr{R}_{\lambda_i} \to \mathscr{R}_{\lambda_i}$. Preto bude

$$u_1 = u_2 = \ldots = u_{k-1} = 0$$

a teda aj $u_k = 0$ a dôkaz bude hotový.
Nech $u \in \mathscr{R}_{\lambda_i} \setminus \{0\}$ a nech

$$(\varphi - \lambda_k \mathrm{id})(u) = 0.$$

Odtiaľ dostávame rovnosť
$$\varphi(u) = \lambda_k u.$$
Nech p je také číslo, že $(\varphi - \lambda_i \mathrm{id})^p(u) = 0$, ale $(\varphi - \lambda_i \mathrm{id})^{p-1}(u) \neq 0$.
Počítajme
$$\begin{aligned}(\varphi - \lambda_i \mathrm{id})^p(u) &= (\varphi - \lambda_i \mathrm{id})^{p-1}(\varphi - \lambda_i \mathrm{id})(u)\\ &= (\varphi - \lambda_i \mathrm{id})^{p-1}(\varphi(u) - \lambda_i u)\\ &= (\varphi - \lambda_i \mathrm{id})^{p-1}(\lambda_k u - \lambda_i u)\\ &= (\lambda_k - \lambda_i)(\varphi - \lambda_i \mathrm{id})^{p-1}(u) \neq 0,\end{aligned}$$
lebo $\lambda_k - \lambda_i \neq 0$ a tiež $(\varphi - \lambda_i \mathrm{id})^{p-1}(u) \neq 0$, čo je ale spor s predpokladom. Preto musí platiť $u = 0$, čo sme potrebovali dokázať.

Ostáva dokázať, že
$$U = \mathscr{R}_{\lambda_1} \oplus \mathscr{R}_{\lambda_2} \oplus \ldots \oplus \mathscr{R}_{\lambda_k}.$$
Vieme určite, že
$$\mathscr{R}_{\lambda_1} \oplus \mathscr{R}_{\lambda_2} \oplus \ldots \oplus \mathscr{R}_{\lambda_k} \subseteq U.$$
Pretože súčet $\mathscr{R}_{\lambda_1} \oplus \mathscr{R}_{\lambda_2} \oplus \ldots \oplus \mathscr{R}_{\lambda_k}$ je direktný, tak z lemy 1.9 a vety o dimenzii prieniku a súčtu platí:
$$\dim(\mathscr{R}_{\lambda_1} \oplus \mathscr{R}_{\lambda_2} \oplus \ldots \oplus \mathscr{R}_{\lambda_k}) = \dim \mathscr{R}_{\lambda_1} + \dim \mathscr{R}_{\lambda_2} + \ldots + \dim \mathscr{R}_{\lambda_k}.$$
K rovnosti
$$\mathscr{R}_{\lambda_1} \oplus \mathscr{R}_{\lambda_2} \oplus \ldots \oplus \mathscr{R}_{\lambda_k} = U$$
nám stačí dokázať, že
$$\dim \mathscr{R}_{\lambda_1} + \dim \mathscr{R}_{\lambda_2} + \ldots + \dim \mathscr{R}_{\lambda_k} = \dim U.$$
Podľa vety 1.15 existuje v U báza $\alpha = (u_1, u_2, \ldots, u_n)$ taká, že
$$(\varphi)_{\alpha,\alpha} = \begin{pmatrix} \lambda_1 & a_{12} & a_{13} & & & & \ldots & & & a_{1n} \\ 0 & \lambda_1 & a_{23} & & & & \ldots & & & a_{2n} \\ & \ddots & \ddots & & & & & & & \\ & & 0 & \lambda_1 & & & & * & & \\ \vdots & & & 0 & \lambda_2 & & & & & \vdots \\ & & & & \ddots & \ddots & & & & \\ & & & & & 0 & \lambda_k & & & \\ & & & & & & \ddots & \ddots & & a_{nn-1} \\ 0 & & & & \ldots & & & & 0 & \lambda_k \end{pmatrix}$$
a λ_i sa vyskytuje v tejto matici práve j_i-krát, čo je jeho algebraická násobnosť. Potrebujeme dokázať, že
$$\dim \mathscr{R}_{\lambda_1} \geq j_1.$$

Pokiaľ dokážeme, že prvých j_1 vektorov bázy α leží v koreňovom podpriestore vlastného čísla λ_1, dôkaz bude hotový. Bázové vektory sú totiž lineárne nezávislé, čiže ak $u_1, u_2, \ldots, u_{j_1}$ ležia v $\mathscr{R}_{\lambda_1}$, tak $\dim \mathscr{R}_{\lambda_1} \geq j_1$. Pretože

$$(\varphi - \lambda_1 \mathrm{id})_{\alpha,\alpha} = \begin{pmatrix} 0 & a_{12} & a_{13} & & \ldots & & a_{1n} \\ 0 & 0 & a_{23} & & \ldots & & a_{2n} \\ & & \ddots & & & * & \\ \vdots & & & 0 & & & \vdots \\ & & & & \lambda_2 - \lambda_1 & & \\ & & & & & \ddots & \\ 0 & & & \ldots & & & \lambda_k - \lambda_1 \end{pmatrix},$$

je

$$(\varphi - \lambda_1 \mathrm{id})(u_1) = 0.$$

Preto $u_1 \in \mathscr{R}_{\lambda_1}$. Pre u_2 dostávame

$$\begin{aligned} (\varphi - \lambda_1 \mathrm{id})^2(u_2) &= (\varphi - \lambda_1 \mathrm{id})(\varphi - \lambda_1 \mathrm{id})(u_2) \\ &= (\varphi - \lambda_1 \mathrm{id})(a_{12} u_1) = 0 \end{aligned}$$

Teda $u_2 \in \mathscr{R}_{\lambda_1}$. Analogicky dokážeme, že $u_3, u_4, \ldots, u_{j_1} \in \mathscr{R}_{\lambda_1}$. □

1.6 Rozklad priestoru pomocou cyklických endomorfizmov

Táto časť sa venuje rozkladu nejakého vektorového priestoru W, na ktorom máme definovaný nilpotentný endomorfizmus $\psi : W \to W$. Najskôr riadne zadefinujeme pojmy cyklického a nilpotentného endomorfizmu. Všimnime si, že endomorfizmus $\varphi - \lambda \mathrm{id}$ zúžený na koreňový podpriestor $\mathscr{R}_\lambda$ je nilpotentný, čiže pod endomorfizmom $\psi : W \to W$ si môžme predstaviť endomorfizmus $\varphi - \lambda \mathrm{id} : \mathscr{R}_\lambda \to \mathscr{R}_\lambda$. Túto konkretizáciu však využijeme až v ďalšej kapitole a teraz sa uspokojíme so všeobecnejším vyjadrením.

Definícia 1.19. Endomorfizmus $\varphi : U \to U$ sa nazýva nilpotentný, ak existuje $k \in \mathbb{N}$ také, že $\varphi^k = 0$. Najmenšie k s touto vlastnosťou nazývame stupeň nilpotentnosti.

Definícia 1.20. Endomorfizmus $\varphi : U \to U$ sa nazýva cyklický, ak v U existuje báza $\alpha = (u_1, u_2, \ldots, u_n)$ taká, že $\varphi(u_1) = 0$, $\varphi(u_2) = u_1$, $\ldots$, $\varphi(u_n) = u_{n-1}$. Matica endomorfizmu v tejto báze má tvar

$$(\varphi)_{\alpha,\alpha} = \begin{pmatrix} 0 & 1 & 0 & \ldots & 0 \\ 0 & 0 & 1 & \ldots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \ldots & 1 \\ 0 & 0 & 0 & \ldots & 0 \end{pmatrix}$$

Veta 1.21. *Majme endomorfizmus* $\psi : W \to W$*, ktorý je nilpotentný. Potom W je direktným súčtom invariantných podpriestorov*

$$W = V_1 \oplus V_2 \oplus \ldots \oplus V_p$$

takých, že $\psi|V_j : V_j \to V_j$ *sú cyklické endomorfizmy.*

Dôkaz. Nech k je stupeň nilpotentnosti endomorfizmu ψ. Teda $\psi^k = 0$.

$$\{0\} = \mathrm{Im}\ \psi^k \subseteq \mathrm{Im}\ \psi^{k-1} \subseteq \mathrm{Im}\ \psi^{k-2} \subseteq \ldots \subseteq \mathrm{Im}\ \psi \subseteq \mathrm{Im}\ \psi^0 = \mathrm{Im}\ \mathrm{id} = W.$$

Dokážeme, že pri inklúziach nenastane nikdy rovnosť. Keby

$$\mathrm{Im}\ \psi^i = \mathrm{Im}\ \psi^{i-1} \neq \{0\},$$

potom

$$\psi(\mathrm{Im}\ \psi^i) = \psi(\mathrm{Im}\ \psi^{i-1})$$
$$\mathrm{Im}\ \psi^{i+1} = \mathrm{Im}\ \psi^i.$$

Odtiaľ vidíme, že

$$\{0\} = \mathrm{Im}\ \psi^k = \mathrm{Im}\ \psi^{k-1} = \ldots = \mathrm{Im}\ \psi^i = \mathrm{Im}\ \psi^{i-1} \neq \{0\},$$

čo je ale spor. Preto bude platiť, že obrazy jednotlivých iterácii endomorfizmu ψ sú vlastnými podmnožinami iterácii nižšieho rádu

$$\{0\} = \mathrm{Im}\ \psi^k \subset \mathrm{Im}\ \psi^{k-1} \subset \mathrm{Im}\ \psi^{k-2} \subset \ldots \subset \mathrm{Im}\ \psi \subset \mathrm{Im}\ \psi^0 = W.$$

Pre jednoduchosť označíme $\mathrm{Im}\ \psi^i$ ako W_i. Čiže

$$\{0\} = W_k \subset W_{k-1} \subset W_{k-2} \subset \ldots \subset W_2 \subset W_1 \subset W_0 = W.$$

Postupne skonštruujeme bázu priestoru W podľa jednotlivých podpriestorov $W_{k-1}, W_{k-2}, \ldots, W_1$.
Nech $(u_1^{k-1}, u_2^{k-1}, \ldots, u_{i_1}^{k-1})$ je báza $W_{k-1} = \psi(W_{k-2})$, ktorej vektory sa zobrazujú do nuly.
Urobíme schému, kde šípky symbolizujú aplikáciu endomorfizmu ψ.

$$\begin{array}{cccc}
0 & 0 & & 0 \\
\uparrow & \uparrow & & \uparrow \\
u_1^{k-1} & u_2^{k-1} & \ldots & u_{i_1}^{k-1} \\
\uparrow & \uparrow & & \uparrow \\
u_1^{k-2} & u_2^{k-2} & \ldots & u_{i_1}^{k-2}
\end{array}$$

Vektory $u_1^{k-2}, u_2^{k-2}, \ldots, u_{i_1}^{k-2} \in W_{k-2}$ sa zobrazia do vyššie uvedených vektorov bázy W_{k-1}.
Dokážeme, že $u_1^{k-1}, u_2^{k-1}, \ldots, u_{i_1}^{k-1}, u_1^{k-2}, u_2^{k-2}, \ldots, u_{i_1}^{k-2}$ sú lineárne nezávislé a teda môžu byť súčasťou bázy W_{k-2}, ktorú hľadáme. Na rovnosť

$$a_1 u_1^{k-1} + a_2 u_2^{k-1} + \ldots + a_{i_1} u_{i_1}^{k-1} + b_1 u_1^{k-2} + b_2 u_2^{k-2} + \ldots + b_{i_1} u_{i_1}^{k-2} = 0$$

aplikujeme endomorfizmus ψ a dostávame

$$b_1u_1^{k-1} + b_2u_2^{k-1} + \ldots + b_{i_1}u_{i_1}^{k-1} = 0.$$

To sú však bázové vektory podpriestoru W_{k-1}, čo znamená, že $b_1 = b_2 = \ldots = b_{i_1} = 0$. Dosadením do pôvodnej rovnice dostávame opäť len kombináciu vektorov bázy W_{k-1} s koeficientami $a_1, a_2, \ldots, a_{i_1}$, ktoré sa preto nutne musia rovnať nule a tým sme dokázali lineárnu nezávislosť všetkých $2i_1$ vektorov. Ostáva doplniť bázu W_{k-2} vhodnými vektormi. Najprv nájdeme nejaké všeobecné vektory $\overline{u}_{i_1+1}^{k-2}, \overline{u}_{i_1+2}^{k-2}, \ldots, \overline{u}_{i_2}^{k-2}$, ktorými doplníme bázu a tie potom upravíme tak, aby sa zobrazovali do nuly. Vieme, že pre všetky $i_1 + 1 \leq j \leq i_2$ sa vektor $\overline{u}_j^{k-2}$ zobrazí do W_{k-1} a teda sa dá napísať ako lineárna kombinácia jeho bázových vektorov, teda že

$$\psi\left(\overline{u}_j^{k-2}\right) = \sum_{r=1}^{i_1} c_{jr}u_r^{k-1}.$$

Preto odčítaním lineárnej kombinácie vektorov $u_1^{k-2}, u_2^{k-2}, \ldots, u_{i_1}^{k-2}$ so získanými koeficientami $c_{j1}, c_{j2}, \ldots, c_{ji_1}$ od vektoru $\overline{u}_j^{k-2}$ získame hľadaný vektor bázy W_{k-2}, ktorý endomorfizmus ψ zobrazí do nuly.

$$u_j^{k-2} = \overline{u}_j^{k-2} - \sum_{r=1}^{i_1} c_{jr}u_r^{k-2}$$

$$\psi\left(u_j^{k-2}\right) = \psi\left(\overline{u}_j^{k-2}\right) - \psi\left(\sum_{r=1}^{i_1} c_{jr}u_r^{k-2}\right) = \sum_{r=1}^{i_1} c_{jr}u_r^{k-1} - \sum_{r=1}^{i_1} c_{jr}u_r^{k-1} = 0$$

Schéma hľadanej bázy W_{k-2} bude vyzerať nasledovne

$$\begin{array}{cccc|ccc}
0 & 0 & & 0 & & & \\
\uparrow & \uparrow & & \uparrow & & & \\
u_1^{k-1} & u_2^{k-1} & \ldots & u_{i_1}^{k-1} & 0 & & 0 \\
\uparrow & \uparrow & & \uparrow & \uparrow & & \uparrow \\
u_1^{k-2} & u_2^{k-2} & \ldots & u_{i_1}^{k-2} & u_{i_1+1}^{k-2} & \ldots & u_{i_2}^{k-2}
\end{array}$$

Overíme, že vektory $u_1^{k-1}, \ldots, u_{i_1}^{k-1}, u_1^{k-2}, \ldots, u_{i_2}^{k-2}$ sú lineárne nezávislé. Rovnosť

$$\sum_{j=1}^{i_1} a_ju_j^{k-1} + \sum_{j=1}^{i_1} b_ju_j^{k-2} + \sum_{j=i_1}^{i_2} d_ju_j^{k-2} = 0$$

môžme napísať ako

$$\sum_{j=1}^{i_1} a_ju_j^{k-1} + \sum_{j=1}^{i_1} b_ju_j^{k-2} + \sum_{j=i_1+1}^{i_2} d_j\overline{u}_j^{k-2} - \sum_{j=i_1}^{i_2}\sum_{r=1}^{i_1} d_jc_{jr}u_r^{k-2} = 0.$$

To sú ale vektory pôvodnej bázy W_{k-2} s koeficientami

a_j pre vektory u_j^{k-1}	kde $1 \leq j \leq i_1$
$b_j - \sum_{j=i_1+1}^{i_2} d_jc_r$ pre vektory u_r^{k-2}	kde $1 \leq r \leq i_1$
d_j pre vektory $\overline{u}_j^{k-2}$	kde $i_1 + 1 \leq j \leq i_2$

Z toho vyplýva, že všetky koeficienty a_j,b_j aj d_j sú nutne nulové a lineárna nezávislosť je dokázaná.

Rovnakým spôsobom určíme bázu W_{k-3}. Bude pozostávať z vektorov bázy W_{k-2}, ďalej z takých, ktoré sa zobrazia do $u_1^{k-2},\dots,u_{i_2}^{k-2}$ a nakoniec z vektorov u_j^{k-3} zobrazujúcich sa do nuly, ktoré získame podobne ako v predchádzajúcom prípade z nejakých ľahko doplniteľných vektorov $\overline{u}_j^{k-3}$ do bázy W_{k-3}:

$$\psi(\overline{u}_j^{k-3}) = \sum_{r=1}^{i_1} c_{jr}u_r^{k-1} + \sum_{r=1}^{i_2} d_{jr}u_r^{k-2},$$

$$u_j^{k-3} = \overline{u}_j^{k-3} - \sum_{r=1}^{i_1} c_{jr}u_r^{k-2} - \sum_{r=1}^{i_2} d_{jr}u_r^{k-3}.$$

Takýmto spôsobom zostavíme postupne bázu priestoru W:

$$\begin{array}{|ccc|ccc|ccc|c|c|}
\hline
0 & & 0 & & & & & & & & \\
\uparrow & & \uparrow & & & & & & & & \\
u_1^{k-1} & \dots & u_{i_1}^{k-1} & 0 & & 0 & & & & & \\
\uparrow & & \uparrow & \uparrow & & \uparrow & & & & & \\
u_1^{k-2} & \dots & u_{i_1}^{k-2} & u_{i_1+1}^{k-2} & \dots & u_{i_2}^{k-2} & 0 & & 0 & & \\
\uparrow & & \uparrow & \uparrow & & \uparrow & \uparrow & & \uparrow & & \\
u_1^{k-3} & \dots & u_{i_1}^{k-3} & u_{i_1+1}^{k-3} & \dots & u_{i_2}^{k-3} & u_{i_2+1}^{k-3} & \dots & u_{i_3}^{k-3} & & \\
 & \vdots & & & \vdots & & & \vdots & & & \\
 & & & & & & & & & & 0 \\
\uparrow & & \uparrow & \uparrow & & \uparrow & \uparrow & & \uparrow & & \uparrow \\
u_1^0 & \dots & u_{i_1}^0 & u_{i_1+1}^0 & \dots & u_{i_2}^0 & u_{i_2+1}^0 & \dots & u_{i_3}^0 & \dots & u_{i_p}^0 \\
\hline
V_1 & \dots & V_{i_1} & V_{i_1+1} & \dots & V_{i_2} & V_{i_2+1} & \dots & V_{i_3} & \dots & V_p \\
\hline
\end{array}$$

V takto zvolenej báze vidíme, že pre všetky $1 \leq i \leq p$ je endomorfizmus ψ zúžený na podpriestore V_i, ktorý je lineárnym obalom vektorov $i-$teho stĺpca, cyklický. □

1.7 Dôkaz Jordanovej vety

Máme riadne zadefinované všetky súvisiace pojmy a dokázané všetky potrebné vety a lemy na to, aby sme mohli prejsť k dôkazu Jordanovej vety.

Dôkaz Jordanovej vety pre endomorfizmy. Vidíme, že podľa predpokladu o spektre vlastných čísel a vete 1.18 môžme vektorový priestor U napísať ako direktný súčet koreňových podpriestorov jednotlivých vlastných čísel:

$$U = \mathscr{R}_{\lambda_1} \oplus \mathscr{R}_{\lambda_2} \oplus \dots \oplus \mathscr{R}_{\lambda_l}.$$

Ďalej vieme, že endomorfizmy $(\varphi - \lambda_i \mathrm{id})^{k_i}$ definujúce koreňové podpriestory $\mathscr{R}_{\lambda_i}$ sú nilpotentné so stupňom nilpotentnosti k_i. Koreňové podpriestory $\mathscr{R}_{\lambda_i}$ potom môžme podľa vety 1.21, kde za ψ berieme $\varphi - \lambda_i \mathrm{id}$, rozložiť na direktný súčet podpriestorov:

$$\mathscr{R}_{\lambda_i} = V_{1,\lambda_i} \oplus V_{2,\lambda_i} \oplus \ldots \oplus V_{p_i,\lambda_i},$$

kde je zúženie endomorfizmu $(\varphi - \lambda_i \mathrm{id})$ na podpriestor V_{j,λ_i} cyklické pre všetky $1 \leq j \leq p_i$. To znamená, že existujú bázy α_{j,λ_i}, v ktorých má matica endomorfizmu na týchto podpriestoroch jednotky nad hlavnou diagonálou a nuly všade inde. Preto môžeme zostaviť maticu endomorfizmu φ na V_{j,λ_i}:

$$(\varphi|_{V_{j,\lambda_i}})_{\alpha_{j,\lambda_i},\alpha_{j,\lambda_i}} = \begin{pmatrix} \lambda_i & 1 & 0 & \ldots & 0 \\ 0 & \lambda_i & 1 & \ldots & 0 \\ \vdots & & \ddots & & \vdots \\ 0 & \ldots & 0 & \lambda_i & 1 \\ 0 & 0 & \ldots & 0 & \lambda_i \end{pmatrix}$$

Podpriestory V_{j,λ_i} sú invariantné vzhľadom k endomorfizmu φ, lebo vektory bázy sa zobrazujú len do lineárnej kombinácie svojho λ_i-násobku a ďalšieho bázového vektora. Preto podľa vety 1.14 môžme maticu endomorfizmu v báze α poskladanej zo všetkých báz α_{j,λ_i} pre $1 \leq j \leq p_i$ a $1 \leq i \leq k$ napísať ako blokovo diagonálnu maticu s Jordanovými bunkami zodpovedajúcimi jednotlivým maticiam endomorfizmu na zúžených endomorfizmoch $(\varphi|_{V_{j,\lambda_i}})_{\alpha_{j,\lambda_i},\alpha_{j,\lambda_i}}$.

Ostáva nám dokázať, že táto matica endomorfizmu je určená jednoznačne až na poradie buniek. To znamená, že JKT nezávisí na báze, čiže v každej báze bude mať rovnaký počet buniek veľkosti $k_i, k_i - 1, \ldots, 1$ pre všetky vlastné čísla λ_i, ktoré sú určené jednoznačne nezávisle od bázy.
Podľa vety 1.21 získame bázu pre JKT, keď položíme $\psi = \varphi - \lambda_i \mathrm{id}|_{\mathscr{R}_{\lambda_i}}$ a podpriestor $W = \mathscr{R}_{\lambda_i}$, ktorá zodpovedá schéme zo strany 16. Príslušné podmnožiny $W_{k_i-1}, W_{k_i-2}, \ldots, W_0$, kde $W_{k_i-1} = \mathrm{Im}(\varphi - \lambda_i \mathrm{id})^{k_i-1}$, sú definované nezávisle od bázy. Preto ak ukážeme, že počet buniek určitej veľkosti závisí len od dimenzii $W_{k_i-1}, W_{k_i-2}, \ldots, W_0$ a nie od výberu ich báz, potom bude dôkaz hotový.
Pri pohľade na schému bázy $W = \mathscr{R}_{\lambda_i}$ z predchádzajúcej strany vidíme, že počet buniek veľkosti k_i pre vlastné číslo λ_i sa rovná $i_1 = \dim W_{k_i-1}$. Počet buniek veľkosti $k_i - 1$ je rovný $i_2 - i_1 = \dim W_{k_i-2} - 2\dim W_{k_i-1}$. Počet buniek veľkosti $k_i - 2$ je $\dim W_{k_i-3} - 2\dim W_{k_i-2} + \dim W_{k_i-1}$. Tu sa vzťah ustáli a všeobecne bude mať tvar

$$\dim W_{k_i-j-1} - 2\dim W_{k_i-j} + \dim W_{k_i-j+1}$$

pre počet buniek veľkosti $k_i - j$, pričom $j = 2, 3, \ldots, k_i - 1$. Takýmto spôsobom určíme počty buniek jednotlivých veľkostí vo všetkých podpriestoroch $\mathscr{R}_{\lambda_i}$ pre $i = 1, 2, \ldots, l$. Vidíme, že všetky skutočne závisia len od dimenzii príslušných podpriestorov $W_{k_i-1}, W_{k_i-2}, \ldots, W_0$ a nie od zvolených báz, čo sme chceli dokázať. $\square$

Kapitola 2

Algebraický dôkaz Jordanovej vety

V druhej kapitole sa budeme venovať dôkazu Jordanovej vety, ktorý využíva algebraické nástroje, najmä polynómy. Budeme postupovať rovnako ako v prvej kapitole. To znamená, že najskôr si v tematických celkoch zadefinujeme dôležité pojmy a vyslovíme dôležité vety, ktoré nám pomôžu postupne sa prepracovať až k samotnému dôkazu Jordanovej vety. V niektorých krokoch upozorníme na paralely s geometrickým dôkazom. Pri dôkaze existencie Jordanovho kanonického tvaru budeme v tejto kapitole čerpať z knihy Ladislava Bicana Lineární algebra a geometrie [1], kde sa tejto téme podrobne venuje 16. a 17. kapitola. Dôkaz jednoznačnosti a spôsob nájdenia JKT nám pomôže ozrejmiť 5. kapitola učebného textu Martina Čadka Lineární algebra a geometrie III [2]. Na začiatku predstavíme niekoľko podstatných viet o polynómoch, ktoré uvedieme bez dôkazu, pričom sa budeme odkazovať na knihu Jiřího Rosického Algebra [3].

2.1 Vety o polynómoch

Ako sme spomenuli v úvode kapitoly, algebraický dôkaz Jordanovej vety je založený najmä na práci s polynómami. Preto si zadefinujeme súvisiace pojmy ako najväčší spoločný deliteľ, či normovaný a ireducibilný polynóm. Ďalej vyslovíme dôležité vety o rôznych vlastnostiach a vzťahoch medzi polynómami, bez ktorých by sme k dôkazu Jordanovej vety nemohli pristúpiť. Množinu všetkých polynómov jednej premennej x s koeficientami z telesa $\mathbb{T}$ budeme označovať symbolom $\mathbb{T}[x]$.

Definícia 2.1. Polynóm s vedúcim koeficientom rovným jednej sa nazýva normovaný polynóm.

Definícia 2.2. Polynóm stupňa väčšieho než 0, ktorý nejde rozložiť na súčin dvoch polynómov nenulového stupňa sa nazýva ireducibilný polynóm.

Veta 2.3. *Nech f, g sú polynómy z $\mathbb{T}[x]$, pričom $f \neq 0$. Potom existujú jednoznačne určené polynómy $\alpha, \beta \in \mathbb{T}[x]$ také, že $g = f\alpha + \beta$, pričom* $\operatorname{st} \beta < \operatorname{st} f$.

Dôkaz. Dôkaz možno nájsť v [3], veta II.5.16. □

Veta 2.4. *Nech $f \in \mathbb{T}[x]$ je polynóm kladného stupňa. Potom môžme tento polynóm rozložiť na súčin $f = af_1^{k_1} f_2^{k_2} \dots f_r^{k_r}$, kde $a \in \mathbb{T}$, $f_1, f_2, \dots, f_r$ sú rôzne normované ireducibilné polynómy z $\mathbb{T}[x]$ a $k_1, k_2, \dots, k_r$ sú kladné celé čísla. Koeficient $a \in \mathbb{T}$ a polynómy $f_1, f_2, \dots, f_r$ sú určené jednoznačne.*

Dôkaz. Dôkaz možno v [3], veta II.5.27. □

Definícia 2.5. Nech $f_1, f_2, \dots, f_r$ sú polynómy v $\mathbb{T}[x]$. Normovaný polynóm $d \in \mathbb{T}[x]$ budeme nazývať najväčším spoločným deliteľom (NSD) polynómov $f_1, f_2, \dots, f_r$, ak bude spĺňať nasledujúce podmienky:

1. d delí f_i pre všetky $i = 1, 2, \dots, r$,
2. pre každý polynóm $k \in \mathbb{T}[x]$, ktorý delí f_i pre všetky $i = 1, 2, \dots, r$ platí, že k delí d.

Veta 2.6 (Bezoutova veta)**.** *Nech f, g sú dva nenulové polynómy z $\mathbb{T}[x]$. Potom existuje práve jeden ich najväčší spoločný deliteľ d. Navyše v $\mathbb{T}[x]$ existujú polynómy β a γ také, že platí*

$$d = \beta f + \gamma g.$$

Dôkaz. Dôkaz možno nájsť v [3], vety II.5.20. a I.3.3. □

Veta 2.7. *Nech $f_1, f_2, \dots, f_r$ sú polynómy v $\mathbb{T}[x]$. Potom existuje práve jeden ich najväčší spoločný deliteľ d. Navyše v $\mathbb{T}[x]$ existujú polynómy $\alpha_1, \alpha_2, \dots, \alpha_r$ také, že platí*

$$d = \alpha_1 f_1 + \alpha_2 f_2 + \dots + \alpha_r f_r.$$

Dôkaz. Dôkaz urobíme indukciou podľa r. Pre $r = 1$ je tvrdenie zrejmé. Nech platí pre $r - 1 \geq 1$ a nech $\mathrm{NSD}(f_1, f_2, \dots, f_r) = d$. Platí

$$d = \mathrm{NSD}(f_1, f_2, \dots, f_r) = \mathrm{NSD}(\mathrm{NSD}(f_1, \dots, f_{r-1}), f_r).$$

Využijeme Bezoutovu vetu a rozložíme d na súčet

$$d = \gamma_1 \mathrm{NSD}(f_1, \dots, f_{r-1}) + \gamma_2 f_r. \tag{2.1}$$

Využijeme indukčný predpoklad a rozpíšeme

$$\mathrm{NSD}(f_1, f_2, \dots, f_{r-1}) = \beta_1 f_1 + \beta_2 f_2 + \dots + \beta_{r-1} f_{r-1}.$$

Dosadíme do (2.1) a dostávame

$$d = \gamma_1 \beta_1 f_1 + \gamma_1 \beta_2 f_2 + \dots + \gamma_1 \beta_{r-1} f_{r-1} + \gamma_2 f_r.$$

Položíme $\gamma_1 \beta_1 = \alpha_1, \gamma_1 \beta_2 = \alpha_2, \dots, \gamma_1 \beta_{r-1} = \alpha_{r-1}, \gamma_2 = \alpha_r$ a dôkaz je hotový. □

Nasledujúce dve tvrdenia vyplývajú práve z Bezoutovej vety.

Veta 2.8. *Nech f a g z $\mathbb{T}[x]$ sú dva polynómy také, že f je ireducibilný a nedelí g. Potom v $\mathbb{T}[x]$ existujú polynómy β a γ také, že $f\beta + g\gamma = 1$.*

Dôkaz. Veta vyplýva priamo z Bezoutovej vety 2.6, kde jedinými deliteľmi polynómu f sú polynóm nultého stupňa a on sám, zatiaľ čo z prepdokladu vidíme, že f nie je deliteľom g. Takže NSD je polynóm nultého stupňa, ktorý sa v normovanom stave rovná jednej. $\square$

Veta 2.9. *Nech polynóm $f \in \mathbb{T}[x]$ je kladného stupňa. Podľa vety 2.4 ho môžme rozložiť na súčin koeficientu z $\mathbb{T}$ a normovaných ireducibilných polynómov z $\mathbb{T}[x]$ takto: $f = af_1^{k_1} f_2^{k_2} \dots f_r^{k_r}$. Pre $i = 1, 2, \dots, r$ označíme symbolom $\overline{f_i}$ súčin všetkých polynómov $f_j^{k_j}$ okrem $f_i^{k_i}$. Potom*

$$f = f_i^{k_i} \overline{f_i}$$

a navyše platí:

1. *pre každé $i = 1, 2, \dots, r$ existujú v $\mathbb{T}[x]$ polynómy β_i, γ_i také, že platí rovnosť $f_i^{k_i}\beta_i + \overline{f_i}\gamma_i = 1$*

2. *v $\mathbb{T}[x]$ existujú prvky $\alpha_1, \alpha_2, \dots, \alpha_r$ také, že platí rovnosť $\overline{f_1}\alpha_1 + \overline{f_2}\alpha_2 + \dots + \overline{f_r}\alpha_r = 1$.*

Dôkaz. Dôkaz prvého bodu vychádza z Bezoutovej vety 2.6, kde $f_i^{k_i}$ a $\overline{f_i}$ nemajú podľa definície spoločného deliteľa a preto ich NSD je rovný 1.
Dôkaz druhého bodu vychádza z vety 2.7, kde z definície $\overline{f_i}$ vidíme, že $\mathrm{NSD}(\overline{f_1}, \overline{f_2}, \dots, \overline{f_r}) = 1$. $\square$

2.2 Vektorový priestor s endomorfizmom ako $\mathbb{T}$[x]-modul

Nasledujúca podkapitola sa venuje definícii modulu. Ukážeme ako pomocou endomorfizmu $\varphi : U \to U$ môžme na U definovať štruktúru $\mathbb{T}[x]$-modulu. Najskôr si však pripomeňme niektoré základné pojmy z algebry, vďaka čomu sa budeme lepšie orientovať v rôznych štruktúrach. Štruktúru $(R, +, \cdot, 1)$ nazývame okruh s jednotkovým prvkom, pokiaľ $(R, +)$ je abelovskou grupou a v $(R, \cdot)$ platí asociativita a existuje v nej jednotkový prvok, pričom v okruhu je násobenie distributívne vzhľadom k sčítaniu. Pripomeňme, že v abelovskej grupe platí medzi prvkami asociativita a komutativita, a existuje v nej nulový aj opačný prvok. Komutatívnym okruhom nazveme okruh, kde operácia násobenia je komutatívna. Komutatívny okruh s inverzným prvkom nazývame telesom a označujeme $\mathbb{T}$. Množina všetkých polynómov $\mathbb{T}[x]$ s koeficientami z telesa $\mathbb{T}$ tvorí komutatívny okruh. Množina všetkých matíc $Mat_n(\mathbb{T})$ s prvkami z telesa $\mathbb{T}$ tvorí nekomutatívny okruh. Abelovskú grupu M nazveme ľavý $R-$modul, pokiaľ existuje zobrazenie $R \times M \to M$ s vlastnosťami:

- $(r_1 + r_2)m = r_1 m + r_2 m$
- $r(m_1 + m_2) = rm_1 + rm_2$
- $r_1(r_2 m) = (r_1 r_2)m$
- $1m = m$

Definícia 2.10. Pokiaľ U je vektorový priestor dimenzie n nad telesom $\mathbb{T}$ a $\varphi : U \to U$ je endomorfizmus na tomto priestore, tak na U môžme definovať štruktúru $\mathbb{T}[x] -$ *modulu*, v ktorom sa násobenie polynómom $f = \sum_{i=0}^{m} a_i x^i$ definuje

$$fu = \sum_{i=0}^{m} a_i \varphi^i(u).$$

Podmodul $\mathbb{T}[x]$-modulu U je podpriestor V taký, že $fv \in V$ pre všetky $f \in \mathbb{T}[x]$ a $v \in V$. Ekvivalentne to znamená, že V je $\varphi-$invariantný podpriestor.

Definícia 2.11. Nech $u \in U \setminus \{0\}$. Normovaný polynóm m_u najmenšieho možného stupňa, pre ktorý platí $m_u u = 0$, sa nazýva minimálny polynóm vektoru u. Normovaný polynóm $m_{U,\varphi}$ najmenšieho možného stupňa, pre ktorý platí $m_{U,\varphi} u = 0$ pre všetky $u \in U$, sa nazýva minimálny polynóm endomorfizmu φ na priestore U.

Veta 2.12. *Buď U vektorový priestor dimenzie n nad telesom $\mathbb{T}$. Potom platí:*

1. *pre každý vektor $u \in U$ existuje minimálny polynóm m_u,*
2. *$gu = 0$ pre nejaký polynóm $g \in \mathbb{T}[x]$, práve keď $m_u | g$,*
3. *existuje minimálny polynóm $m_{U,\varphi}$ priestoru U,*
4. *$gu = 0$ pre nejaký polynóm g a pre každé $u \in U$, práve keď $m_{U,\varphi} | g$.*

Dôkaz. 1. Nech U je vektorový priestor dimenzie n. Majme ľubovoľný vektor $u \in U$. Vektory $u, \varphi(u), \ldots, \varphi^n(u)$ budú lineárne závislé, keďže ich počet je väčší ako dimezia U a preto $\sum_{i=0}^{n} a_i \varphi^i(u) = 0$ pre nejaké nie všetky nulové $a_0, a_1, \ldots, a_n$. Potom je polynóm $f = \sum_{i=0}^{n} a_i x^i$ nenulový a $fu = \sum_{i=0}^{n} a_i \varphi^i(u) = 0$. Stačí nájsť normovaný polynóm najmenšieho stupňa splňujúci podmienku $fu = 0$.
2. Najprv ak $m_u | g$, tak $g = m_u h$ pre nejaký polynóm $h \in \mathbb{T}[x]$ a $gu = hm_u u = 0$. Naopak ak $gu = 0$, tak podľa vety 2.3 existujú polynómy $q, r \in \mathbb{T}[x]$, pre ktoré platí $g = m_u q + r$ a st $r <$st m_u. Po vynásobení oboch strán vektorom u a drobných úpravách dostaneme $ru = gu - qm_u u = 0$, odkiaľ vidíme, že $r = 0$, lebo v opačnom prípade by mal tento polynóm nižší stupeň ako m_u, čo je v spore s definíciou. Preto $g = m_u q$ a teda $m_u | g$.
3. Nech $(u_1, u_2, \ldots, u_n)$ je báza priestoru U a nech polynóm $f = m_{u_1} m_{u_2} \ldots m_{u_n} = m_{u_i} \overline{m}_{u_i}$. Ľubovoľný vektor $u \in U$ môžme napísať ako $u = \sum_{i=1}^{n} a_i u_i$. Potom $fu = \sum_{i=1}^{n} f(a_i u_i) = \sum_{i=1}^{n} m_{u_i} \overline{m}_{u_i}(a_i u_i) = 0$, keďže $m_{u_i} u_i = 0$ pre všetky $i = 1, 2, \ldots, n$. Stačí opäť nájsť normovaný polynóm s najnižším stupňom s danou vlastnosťou.
4. Tento dôkaz je analogický s dôkazom 2. bodu. □

Veta 2.13 (Zornova lema)**.** *Pokiaľ v (čiastočne) usporiadanej množine ku každej lineárne usporiadanej podmnožine existuje maximálny prvok, potom v tejto množine existuje maximálny prvok.*

Dôkaz. Dôkaz možno nájsť v [5], tvrdenie II.8.1. □

Definícia 2.14. Najmenší $\mathbb{T}[x]-$podmodul modulu U obsahujúci vektor u definujeme ako

$$\langle u \rangle = \{su \in U,\ s \in \mathbb{T}[x]\}.$$

Lema 2.15. *Nech f je nejaký ireducibilný polynóm v $\mathbb{T}[x]$ a k nejaké prirodzené číslo. Položme $M \subset U$ ako*

$$M = \{u \in U | \ f^k u = 0\}.$$

Potom M je $\mathbb{T}[x]-$podmodul.

Dôkaz. Nech vektor u leží v M a nech g je nejaký polynóm z $\mathbb{T}[x]$, potom

$$f^k gu = gf^k u = g0 = 0$$

a preto $gu \in M$. □

Veta 2.16. *Nech f je ireducibilný normovaný polynóm nad telesom $\mathbb{T}$. Majme nenulový podpriestor $M \subset U$, ktorý je $\mathbb{T}[x]$-podmodulom a platí preň:*

$$f^k M = \{f^k w; \ w \in M\} = 0 \tag{2.2}$$

kde k je prirodzené číslo. Potom v M existujú vektor u a podmodul N také, že môžme M rozložiť na direktný súčet

$$M = \langle u \rangle \oplus N.$$

Ak vezmeme najmenšie k s vlastnosťou (2.2), môžeme $u \in M$ zvoliť ako vektor s vlastnosťou $f^{k-1}u \neq 0$ a podmodul N ako maximálny podmodul v M neobsahujúci vektor $f^{k-1}u$.

Poznámka. Podmodul N existuje vďaka Zornovej leme 2.13.

Lema 2.17. *Zvoľme f, M, k, u a N rovnako ako v predchádzajúcej vete 2.16. Položme $v = f^{k-1}u$. Pre ľubovoľný polynóm s sú nasledujúce tvrdenia ekvivalentné*

1. *$sv \in N$,*
2. *f delí s,*
3. *$sv = 0$.*

Dôkaz. (2) implikuje (3): ak f delí s, tak s môžme napísať ako $s = hf$. Potom $sv = hfv = hf^k u = 0$.
(3) implikuje (1) je zrejmé.
(1) implikuje (2) dokážeme obmenenou implikáciou. Ak f nedelí s, potom vďaka ireducibilite f použijeme rovnosť $\beta f + \gamma s = 1$ z vety 2.8. Vieme teda, že $v = \beta f v + \gamma s v = \gamma s v$, keďže $\beta f v = \beta f^k u = 0$. Ak by $sv \in N$, tak potom by aj $v = \gamma s v \in N$, čo je spor s definíciou v. □

Dôkaz vety 2.16. Najskôr dokážeme, že

$$\langle u \rangle \cap N = 0.$$

K tomu stačí ukázať, že ak $a \in \langle u \rangle \cap N$, tak

$$f^i a = 0$$

postupne pre $i = k, k-1, \dots, 0$. Pre $i = k$ je platnosť zrejmá. Nech platí tiež pre $0 < i < k$. Vektor a leží v $\langle u \rangle \cap N$, čo znamená, že ho môžme napísať ako $a = ru$ pre nejaké $r \in \mathbb{T}[x]$ a zároveň vieme, že tento vektor leží v N, čiže

$$a = ru \in N.$$

Ak $f^i a = f^i ru = 0$, tak podľa vety 2.12 o vlastnostiach minimálneho polynómu platí, že f^k delí $f^i r$, čo znamená, že $f^i r = f^k t$, kde $t \in \mathbb{T}[x]$. Po úprave dostaneme vzťah $r = f^{k-i} t$. S jeho pomocou už ľahko dokážeme, že $f^{i-1} a = 0$, lebo

$$f^{i-1} a = f^{i-1} ru = f^{i-1} f^{k-i} tu = f^{k-1} tu = tv \in N$$

a $ru \in N$. Ak použijeme lemu 2.17, dostaneme, že $f^{i-1} a = tv = 0$.

Ostáva dokázať, že

$$M = \langle u \rangle + N.$$

Túto časť dokážeme sporom. Predpokladajme, že $\langle u \rangle + N$ je vlastnou podmnožinou M. Hľadáme prvok $b \in M \setminus (\langle u \rangle + N)$ taký, že $fb \in \langle u \rangle + N$. Nech $a \in M \setminus (\langle u \rangle + N)$. Z definície 2.16 vieme, že $f^k a = 0$ a teda určite existuje prirodzené číslo l také, že $f^l a \in \langle u \rangle + N$ a $f^{l-1} a \notin \langle u \rangle + N$. Položme $f^{l-1} a = b$. Máme teda požadovaný prvok taký, že $b \in M \setminus (\langle u \rangle + N)$ a $fb \in \langle u \rangle + N$, ktorý môžme napísať ako

$$fb = tu + w$$

pre nejaké $w \in N$ a $t \in \mathbb{T}[x]$. Preto

$$0 = f^k b = f^{k-1} tu + f^{k-1} w = tv + f^{k-1} w,$$

čo nám dáva rovnosť $tv = -f^{k-1} w \in N$. Preto podľa lemy 2.17 f delí t a teda $t = fq$ pre nejaké $q \in \mathbb{T}[x]$, čo využijeme vo vzťahu $fb = tu + w$ a nahradíme ho rovnicou $fb = fqu + w$. Dostávame

$$f(b - qu) = w \in N, \tag{2.3}$$

pričom vektor $b - qu$ neleží v $\langle u \rangle + N$, keďže $b \notin \langle u \rangle + N$. Potom logicky $b - qu$ nemôže ležať v N. Preto N je nutne vlastnou podmnožinou $\langle b - qu \rangle + N$ a keďže je zároveň maximálnym podmodulom modulu M vzhľadom k $v \notin N$, tak dostávame $v \in \langle b - qu \rangle + N$. Vektor v môžme napísať ako

$$v = p(b - qu) + w' \tag{2.4}$$

pre nejaké $p \in \mathbb{T}[x]$ a $w' \in N$. Uvažujme teraz dva prípady - prvý, že f delí p a druhý, že f nedelí p. V prvom rozkladáme p na súčin fr pre nejaké vhodné $r \in \mathbb{T}[x]$. Potom pomocou (2.3) a (2.4) dostaneme, že

$$v = fr(b - qu) + w' = rw + w',$$

kde $w, w' \in N$, čo znamená, že $v \in N$ a dostávame spor. V druhom prípade ak f nedelí p, tak s využitím ireducibility f je podľa vety 2.8 $f\beta + p\gamma = 1$ pre vhodné $\beta, \gamma \in \mathbb{T}[x]$, čo spolu s (2.3) a (2.4) využijeme k úprave vzťahu $b - qu$.

$$b - qu = \beta f(b - qu) + \gamma p(b - qu) = \beta w + \gamma v - \gamma w',$$

kde $v \in \langle u \rangle$ a $w, w' \in N$, a preto $b - qu \in \langle u \rangle + N$, čo je spor s tým, že $b \notin \langle u \rangle + N$. $\square$

2.3 Definícia a vlastnosti λ-matíc

Ako sme spomenuli v predchádzajúcej časti, $R = Mat_n(\mathbb{T})$ tvorí nekomutatívny okruh a v $R[\lambda]$ dostávame polynómy s koeficientami v tvare matíc. Každý takýto polynóm

$$\mathbf{A}(\lambda) = \mathbf{A}_0 + \lambda \mathbf{A}_1 + \ldots + \lambda^k \mathbf{A}_k$$

môžme súčasne chápať ako maticu $n \times n$ s prvkami, ktoré sú polynómami z $\mathbb{T}[x]$. Platí

$$Mat_n(\mathbb{T})[\lambda] \cong Mat_n(\mathbb{T}[\lambda]).$$

Príkladom takéhoto polynómu je charakteristická matica $\mathbf{A} - \lambda \mathbf{E}$, kde absolútnym členom je matica $\mathbf{A}$ a vedúcim koeficientom (koeficient u najvyššej mocniny) polynómu so stupňom 1 je diagonálna matica s -1 na diagonále. Ukážeme vlastnosti takýchto polynómov a spôsob ako upravovať matice, ktorých prvkami sú práve polynómy. Definujeme si pojmy ako ekvivalencia matíc a kanonická matica, ktoré použijeme k dôkazu jednoznačnosti Jordanovho kanonického tvaru.

Definícia 2.18. Štvorcová matica $\mathbf{A}(\lambda) = (a_{ij}(\lambda))$, kde prvky $a_{ij}(\lambda)$ sú nejaké polynómy s neznámou λ nad telesom $\mathbb{T}$ sa nazýva $\lambda - matica$ nad telesom $\mathbb{T}$. Takúto maticu môžme rozložiť na súčet

$$\mathbf{A}(\lambda) = \mathbf{A}_0 + \lambda \mathbf{A}_1 + \lambda^2 \mathbf{A}_2 + \ldots + \lambda^k \mathbf{A}_k,$$

kde $\mathbf{A}_0, \mathbf{A}_1, \ldots, \mathbf{A}_k$ sú matice nad telesom $\mathbb{T}$. Pre ľubovoľnú štvorcovú maticu $\mathbf{B}$ môžme definovať maticu $\mathbf{L}_\mathbf{A}(\mathbf{B})$ nad telesom $\mathbb{T}$, ktorá vznikne dosadením matice $\mathbf{B}$ do polynómu $\mathbf{A}(\lambda)$ za λ zľava.

$$\mathbf{L}_\mathbf{A}(\mathbf{B}) = \mathbf{A}_0 + \mathbf{B}\mathbf{A}_1 + \ldots + \mathbf{B}^k \mathbf{A}_k.$$

Analogicky definujeme

$$\mathbf{P}_\mathbf{A}(\mathbf{B}) = \mathbf{A}_0 + \mathbf{A}_1\mathbf{B} + \ldots + \mathbf{A}_k\mathbf{B}^k$$

pre dosadenie matice $\mathbf{B}$ do $\mathbf{A}(\lambda)$ sprava.

Lema 2.19. *Stupeň súčinu dvoch nenulových polynómov s maticami ako koeficientami sa rovná súčtu ich stupňov, pokiaľ v aspoň jednom polynóme je vedúci koeficient regulárna matica.*

Dôkaz. Je zrejmé, že stupeň súčinu dvoch nenulových polynómov sa rovná súčtu ich stupňov, pokiaľ súčin vedúcich koeficientov, v našom prípade nenulových matíc $\mathbf{A}$ a $\mathbf{B}$ pri vedúcich členoch, nie je nulová matica. Dôkaz urobíme sporom. Nech súčin matíc $\mathbf{AB} = 0$. Predpokladajme, že $\mathbf{A}$ je regulárna, z čoho vyplýva, že k nej existuje inverzná matica $\mathbf{A}^{-1}$. Zároveň platí

$$\mathbf{B} = \mathbf{A}^{-1}(\mathbf{AB}) = \mathbf{A}^{-1}0 = 0,$$

čo je ale spor s predpokladom. Analogicky dokážeme pre $\mathbf{B}$ regulárnu. $\square$

Veta 2.20. *Nech $\mathbf{A}(\lambda)$ je štvorcová λ-matica so stupňom aspoň 1 nad telesom $\mathbb{T}$ a $\mathbf{B}$ je ľubovoľná matica nad telesom $\mathbb{T}$, potom existuje práve jedna λ-matica $\mathbf{C}(\lambda)$ a práve jedna matica $\mathbf{D}$ nad telesom $\mathbb{T}$ tak, že*

$$\mathbf{A}(\lambda) = (\mathbf{B} - \lambda \mathbf{E})\mathbf{C}(\lambda) + \mathbf{D},$$

pričom $\mathbf{D} = \mathbf{L}_\mathbf{A}(\mathbf{B})$. Analogicky veta platí pre násobenie polynómom $\mathbf{B} - \lambda \mathbf{E}$ sprava, pričom $\mathbf{D} = \mathbf{P}_\mathbf{A}(\mathbf{B})$.

Dôkaz. K dôkazu využijeme formulu $a^i - b^i = (a-b)(a^{i-1} + a^{i-2}b + \ldots + ab^{i-2} + b^{i-1})$, ktorú aplikujeme na výraz $\mathbf{B}^i - \lambda^i\mathbf{E}$, čo môžme, keďže $\mathbf{B}$ a $\mathbf{E}$ komutujú.

$$\mathbf{B}^i - \lambda^i\mathbf{E} = (\mathbf{B} - \lambda\mathbf{E})(\mathbf{B}^{i-1} + \lambda\mathbf{B}^{i-2} + \lambda^2\mathbf{B}^{i-3} + \ldots + \lambda^{i-2}\mathbf{B} + \lambda^{i-1}\mathbf{E}).$$

Odtiaľ po odčítaní $\mathbf{L}_\mathbf{A}(\mathbf{B})$ od $\mathbf{A}(\lambda)$ dostávame

$$\mathbf{A}(\lambda) - \mathbf{L}_\mathbf{A}(\mathbf{B}) = \sum_{i=1}^{k} \lambda^i\mathbf{A}_i - \sum_{i=1}^{k} \mathbf{B}^i\mathbf{A}_i = -\sum_{i=1}^{k} (\mathbf{B}^i - \lambda^i\mathbf{E})\mathbf{A}_i = (\mathbf{B} - \lambda\mathbf{E})\mathbf{C}(\lambda)$$

pre vhodnú $\lambda-$maticu $\mathbf{C}(\lambda)$. Ostáva dokázať jednoznačnosť. Uvažujme, že

$$\mathbf{A}(\lambda) = (\mathbf{B} - \lambda\mathbf{E})\mathbf{C}(\lambda) + \mathbf{L}_\mathbf{A}(\mathbf{B})$$

a zároveň

$$\mathbf{A}(\lambda) = (\mathbf{B} - \lambda\mathbf{E})\mathbf{C}_1(\lambda) + \mathbf{D}.$$

Po odčítaní týchto dvoch rovníc dostávame

$$\mathbf{D} - \mathbf{L}_\mathbf{A}(\mathbf{B}) = (\mathbf{B} - \lambda\mathbf{E})(\mathbf{C}(\lambda) - \mathbf{C}_1(\lambda)),$$

kde vidíme, že na ľavej strane rovnice máme $\lambda-$maticu stupňa 0, pričom podľa lemy 2.19 by pri nerovnosti $\mathbf{C}(\lambda) \neq \mathbf{C}_1(\lambda)$ na pravej strane bola λ-matica so stupňom väčším ako 0, keďže vedúcim koeficientom v polynóme $\mathbf{B} - \lambda\mathbf{E}$ je matica s -1 na diagonále, ktorá je regulárna. Musí teda platiť $\mathbf{C}(\lambda) = \mathbf{C}_1(\lambda)$ a odtiaľ tiež platí $\mathbf{D} = \mathbf{L}_\mathbf{A}(\mathbf{B})$. Analogicky dokážeme pre násobenie $\mathbf{B} - \lambda\mathbf{E}$ sprava. □

Veta 2.21 (Hamiltonova-Cayleyova)**.** *Nech* $\mathbf{A}$ *je štvorcová matica s prvkami z telesa* $\mathbb{T}$ *a* $g(\lambda) = |\mathbf{A} - \lambda\mathbf{E}|$ *je jej charakteristický polynóm. Potom po dosadení matice* $\mathbf{A}$ *za* λ *do polynómu* $g(\lambda)$ *platí* $g(\mathbf{A}) = 0$.

Dôkaz. Maticu $g(\lambda)\mathbf{E}$ môžme podľa predchádzajúcej vety napísať ako

$$g(\lambda)\mathbf{E} = (\mathbf{A} - \lambda\mathbf{E})\mathbf{C}(\lambda) + g(\mathbf{A}).$$

Pokiaľ za $\mathbf{C}(\lambda)$ zvolíme adjungovanú maticu k $\mathbf{A} - \lambda\mathbf{E}$, tak z vlastnosti adjungovanej matice $(\mathbf{A} - \lambda\mathbf{E})\mathbf{C}(\lambda) = \det(\mathbf{A} - \lambda\mathbf{E})\mathbf{E} = g(\lambda)\mathbf{E}$ a z jednoznačnosti dokázanej vo vete 2.20 vyplýva rovnosť $g(\mathbf{A}) = 0$. □

Definícia 2.22. Riadkové a stĺpcové elementárne úpravy λ-matíc definujeme nasledovne:

1. vynásobenie riadku (stĺpca) nenulovým číslom z telesa $\mathbb{T}$,
2. výmena riadkov (stĺpcov),
3. pričítanie polynomiálneho násobku $j-$teho riadku (stĺpca)k $i-$temu riadku (stĺpcu), pričom $i \neq j$.

Riadkové elementárne operácie môžme realizovať násobením maticou $\mathbf{P}(\lambda)$ zľava, pričom $\det\mathbf{P}(\lambda) \in \mathbb{T} \setminus \{0\}$. O matici s touto vlastnosťou hovoríme, že je invertibilná. Stĺpcové operácie môžme realizovať zasa násobením invertibilnou maticou $\mathbf{Q}(\lambda)$ sprava.

Definícia 2.23. Matica $\mathbf{A}(\lambda)$ je ekvivalentná s maticou $\mathbf{B}(\lambda)$, pokiaľ maticu $\mathbf{B}(\lambda)$ dostaneme z matice $\mathbf{A}(\lambda)$ elementárnymi operáciami, čiže existujú invertibilné matice $\mathbf{P}(\lambda)$ a $\mathbf{Q}(\lambda)$ také, že

$$\mathbf{B}(\lambda) = \mathbf{P}(\lambda)\mathbf{A}(\lambda)\mathbf{Q}(\lambda).$$

Veta 2.24. *Matice $\mathbf{A}$ a $\mathbf{B}$ sú podobné práve vtedy, keď matice $\mathbf{A} - \lambda\mathbf{E}$ a $\mathbf{B} - \lambda\mathbf{E}$ sú ekvivalentné.*

Dôkaz. Nech sú matice $\mathbf{A}$ a $\mathbf{B}$ podobné. Potom existuje invertibilná matica $\mathbf{P}$ taká, že

$$\mathbf{B} = \mathbf{P}\mathbf{A}\mathbf{P}^{-1}$$

a tiež

$$\lambda\mathbf{E} = \mathbf{P}(\lambda\mathbf{E})\mathbf{P}^{-1}.$$

Odtiaľ

$$\mathbf{B} - \lambda\mathbf{E} = \mathbf{P}(\mathbf{A} - \lambda\mathbf{E})\mathbf{P}^{-1}.$$

Nech sú matice $\mathbf{A} - \lambda\mathbf{E}$ a $\mathbf{B} - \lambda\mathbf{E}$ ekvivalentné. Potom existujú invertibilné matice $\mathbf{P}(\lambda)$ a $\mathbf{Q}(\lambda)$ také, že

$$\mathbf{B} - \lambda\mathbf{E} = \mathbf{P}(\lambda)(\mathbf{A} - \lambda\mathbf{E})\mathbf{Q}(\lambda).$$

Podľa vety 2.20 rozpíšeme

$$\mathbf{P}(\lambda) = (\mathbf{B} - \lambda\mathbf{E})\mathbf{P}_1 + \mathbf{P}_0$$
$$\mathbf{Q}(\lambda) = \mathbf{Q}_1(\mathbf{B} - \lambda\mathbf{E}) + \mathbf{Q}_0.$$

Pomocou posledných troch rovníc postupne upravujeme výraz

$$\begin{aligned}
\mathbf{P}_0(\mathbf{A} - \lambda\mathbf{E})\mathbf{Q}_0 &= \big(\mathbf{P}(\lambda) - (\mathbf{B} - \lambda\mathbf{E})\mathbf{P}_1\big)(\mathbf{A} - \lambda\mathbf{E})\big(\mathbf{Q}(\lambda) - \mathbf{Q}_1(\mathbf{B} - \lambda\mathbf{E})\big) \\
&= \big(\mathbf{P}(\lambda)(\mathbf{A} - \lambda\mathbf{E})\mathbf{Q}(\lambda)\big) - \big((\mathbf{B} - \lambda\mathbf{E})\mathbf{P}_1(\mathbf{A} - \lambda\mathbf{E})\mathbf{Q}(\lambda)\big) - \\
&\quad - \big(\mathbf{P}(\lambda)(\mathbf{A} - \lambda\mathbf{E})\mathbf{Q}_1(\mathbf{B} - \lambda\mathbf{E})\big) + \big((\mathbf{B} - \lambda\mathbf{E})\mathbf{P}_1(\mathbf{A} - \lambda\mathbf{E})\mathbf{Q}_1(\mathbf{B} - \lambda\mathbf{E})\big) \\
&= (\mathbf{B} - \lambda\mathbf{E}) - \big((\mathbf{B} - \lambda\mathbf{E})\mathbf{P}_1\mathbf{P}^{-1}(\lambda)(\mathbf{B} - \lambda\mathbf{E})\big) - \\
&\quad - \big((\mathbf{B} - \lambda\mathbf{E})\mathbf{Q}^{-1}(\lambda)\mathbf{Q}_1(\mathbf{B} - \lambda\mathbf{E}) + \big((\mathbf{B} - \lambda\mathbf{E})\mathbf{P}_1(\mathbf{A} - \lambda\mathbf{E})\mathbf{Q}_1(\mathbf{B} - \lambda\mathbf{E})\big) \\
&= (\mathbf{B} - \lambda\mathbf{E})\Big(\mathbf{E} - \big(\mathbf{P}_1\mathbf{P}^{-1}(\lambda) - \mathbf{Q}^{-1}(\lambda)\mathbf{Q}_1 + \mathbf{P}_1(\mathbf{A} - \lambda\mathbf{E})\mathbf{Q}_1\big)(\mathbf{B} - \lambda\mathbf{E})\Big)
\end{aligned}$$

Keďže pôvodný výraz $\mathbf{P}_0(\mathbf{A} - \lambda\mathbf{E})\mathbf{Q}_0$ je $\lambda-$matica so stupňom 1, rovnako ako aj matica $\mathbf{B} - \lambda\mathbf{E}$, tak výraz vo veľkej zátovrke v poslednom kroku musí mať stupeň 0. To platí iba v prípade, že v jeho druhom sčítanci maticu $\mathbf{B} - \lambda\mathbf{E}$ so stupňom 1 vynásobíme nulovou maticou a ostane v ňom iba jednotková matica, odkiaľ dostaneme rovnosť

$$\mathbf{P}_0(\mathbf{A} - \lambda\mathbf{E})\mathbf{Q}_0 = \mathbf{B} - \lambda\mathbf{E}.$$

Po roznásobení a porovnaní koeficientov pri λ^0 a λ^1 dostaneme

$$\mathbf{P}_0\mathbf{A}\mathbf{Q}_0 = \mathbf{B}$$

a dôležitú rovnosť

$$\mathbf{P}_0\mathbf{Q}_0 = \mathbf{E},$$

kde vidíme, že $\mathbf{Q}_0 = \mathbf{P}_0^{-1}$ a teda platí dokazovaný vzťah podobnosti matíc $\mathbf{A}$ a $\mathbf{B}$

$$\mathbf{P}_0\mathbf{A}\mathbf{P}_0^{-1} = \mathbf{B}.$$

□

Definícia 2.25. O $\lambda-$matici $\mathbf{K}(\lambda)$ hovoríme, že je v kanonickom tvare, pokiaľ

$$\mathbf{K}(\lambda) = \left(\begin{array}{cccccc} p_1(\lambda) & 0 & 0 & & \dots & 0 \\ 0 & p_2(\lambda) & 0 & & \dots & 0 \\ \vdots & \vdots & \ddots & & & \vdots \\ 0 & 0 & \dots & p_l(\lambda) & \dots & 0 \\ \hline 0 & & \dots & & 0 \quad \dots & 0 \\ \vdots & & & & \ddots & \vdots \\ 0 & & \dots & & & 0 \end{array}\right),$$

kde $l \leq n$ a nenulové polynómy $p_i(\lambda)$ sú normované a platí pre ne, že $p_i(\lambda)$ delí $p_{i+1}(\lambda)$ pre $i = 1, 2, \dots, l-1$.

Lema 2.26. *Každú štvorcovú $\lambda-$maticu môžme pomocou riadkových a stĺpcových elementárnych úprav previesť na maticu v kanonickom tvare.*

Dôkaz. Nájdenie kanonického tvaru matice je modifikáciou Gaussovej eliminačnej metódy. Dôkaz urobíme indukciou.
Pre maticu 1×1 je platnosť lemy zrejmá. Nech tvrdenie platí pre $(n-1) \times (n-1)$. Uvažujme nenulovú maticu $\mathbf{A}(\lambda)$ tvaru $n \times n$. Pomocou elementárnej operácie výmeny riadkov a stĺpcov presunieme na pozíciu $a_{11}(\lambda)$ nenulový polynóm s najnižším stupňom. Potom vynulujeme všetky prvky na zvyšných pozíciach v prvom stĺpci matice. Buď sú tieto polynómy $a_{i1}(\lambda)$ deliteľné polynómom $a_{11}(\lambda)$ a stačí iba odčítať príslušný $q(\lambda)$-násobok prvého riadku matice, alebo deliteľné nie sú a vtedy využijeme vzťah

$$a_{i1}(\lambda) = q(\lambda)a_{11}(\lambda) + \overline{a}_{11}(\lambda),$$

pričom st $\overline{a}_{11}(\lambda) <$ st $a_{11}(\lambda)$. Od $i-$teho riadku odčítame $q(\lambda)-$násobok prvého riadku a potom tieto riadky vymeníme. Na pozícii $i = 1, j = 1$ máme nový nenulový polynóm najmenšieho stupňa $\overline{a}_{11}(\lambda)$. Postup opakujeme, kým polynóm v ľavom hornom rohu nedelí polynóm $a_{i1}(\lambda)$. Potom pokračujeme už spomínaným postupom odčítania príslušného $q(\lambda)-$ násobku prvého riadku od $i-$teho riadku a na pozícii $a_{i1}(\lambda)$ dostávame nulu. Rovnako vynulujeme aj prvý riadok pre $j \neq 1$. Dostávame maticu

$$\left(\begin{array}{c|ccc} a_{11}(\lambda) & 0 & \dots & 0 \\ \hline 0 & & & \\ \vdots & & \overline{\mathbf{A}}(\lambda) & \\ 0 & & & \end{array}\right)$$

Rovnako postupujeme pre maticu $\overline{\mathbf{A}}$. Najskôr však musíme ošetriť dôležitú vlastnosť kanonického tvaru – deliteľnosť polynómu p_i polynómom p_{i-1}. Stačí, aby prvok a_{11} delil

všetky nenulové prvky matice $\overline{\mathbf{A}}(\lambda)$. Z doterajšieho postupu je zrejmé, že buď $a_{ij} = 0$ alebo st $a_{11}(\lambda) \leq a_{ij}(\lambda)$ pre všetky $a_{ij}(\lambda)$ z $\mathbf{A}(\lambda)$. Pre druhý prípad opäť využijeme, že $a_{ij}(\lambda) = q(\lambda)a_{11}(\lambda) + \overline{a}_{11}(\lambda)$. Pokiaľ $\overline{a}_{11}(\lambda) \neq 0$, tak tento polynóm už spomínanými úpravami dostaneme na pozíciu $i = 1, j = 1$, vynulujeme 1. riadok a 1. stĺpec a postup opakujeme, kým $a_{11}(\lambda)$ nedelí všetky nenulové prvky matice $\overline{\mathbf{A}}(\lambda)$.
Teraz už môžme použiť indukčný predpoklad a takýmto spôsobom upraviť maticu $\overline{\mathbf{A}}(\lambda)$. Dostaneme maticu v tvare

$$\mathbf{K}(\lambda) = \begin{pmatrix} p_1(\lambda) & 0 & 0 & & \dots & 0 \\ 0 & p_2(\lambda) & 0 & & \dots & 0 \\ & & \ddots & & & \\ & & & p_l(\lambda) & & \\ \vdots & & & & 0 & \vdots \\ & & & & & \ddots \\ 0 & & \dots & & & 0 \end{pmatrix},$$

kde p_i delí p_{i+1} pre $i = 1, 2, \dots, l-1$, keďže $a_{11} = p_1$ delilo všetky nenulové prvky $\overline{\mathbf{A}}(\lambda)$ a musí ich teda deliť aj po elementárnych úpravách. Takže p_1 delí p_2 a vďaka indukcii môžme tento vzťah zobecniť. $\square$

Veta 2.27. *Štvorcové matice $\mathbf{A}(\lambda)$ a $\mathbf{B}(\lambda)$ veľkosti n sú ekvivalentné práve vtedy, keď majú rovnaký kanonický tvar.*

Dôkaz. Označme najväčší normovaný spoločný deliteľ všetkých minorov stupňa k v matici $\mathbf{A}(\lambda)$ ako d_k^A, pričom v prípade, že sú všetky minory nulové sa $d_k^A = 0$. Z definície kanonického tvaru matice ľahko zistíme, že ak je matica $\mathbf{A}$ v kanonickom tvare, tak

$$\begin{aligned} p_1 &= d_1^A \\ p_k &= \frac{d_k^A}{d_{k-1}^A}, \qquad \text{pokiaľ } d_{k-1}^A \neq 0, \\ p_k &= 0 \qquad \text{práve vtedy, keď } d_k^A = 0 \end{aligned}$$

lebo $d_1^A = NSD(p_1, p_2, \dots, p_l, 0)$, teda podľa definície to bude práve polynóm p_1. Pre $d_2^A = NSD(p_i p_j, 0)$, kde najmenším bude minor matice z prvých dvoch riadkov a stĺpcov $p_1 p_2$, odkiaľ dostávame $p_2 = \frac{d_2^A}{d_1^A}$. Rovnakým spôsobom postupujeme pre d_i^A až do $i = l$.
Ak dokážeme, že $d_k^A = d_k^B$ pre všetky $k = 1, 2, \dots, l$, tak ich kanonický tvar bude rovnaký. Stačí teda dokázať, že elementárne operácie nemenia d_k^A. Keďže d_k^A je normovaný polynóm, tak vynásobenie riadku (stĺpca) skalárom alebo výmena dvoch riadkov (stĺpcov) ho určite nezmení. Pri pričítaní $q(\lambda)$-násobku jedného riadku (stĺpca) k druhému môžme ľubovoľný minor stupňa k takto vzniknutej matice, označíme ju $\mathbf{A_2}$, rozložiť na súčet

$$\det \mathbf{M}_1 + q(\lambda) \det \mathbf{M}_2,$$

kde minory $\det \mathbf{M}_1$ a $\det \mathbf{M}_2$ sú minormi stupňa k pôvodnej matice $\mathbf{A}$. d_k^A delí oba sčítance a preto delí aj ich súčet. To znamená, že d_k^A musí deliť aj $d_k^{A_2}$. Podobnými elementárnymi operáciami prevedieme maticu $\mathbf{A_2}$ na pôvodný tvar $\mathbf{A}$, pričom rovnako bude platiť, že $d_k^{A_2}$ delí d_k^A. Odtiaľ

$$d_k^{A_2} = d_k^A.$$

□

Definícia 2.28. Nenulový normovaný polynóm $m \in \mathbb{T}[\lambda]$ nazveme minimálnym polynómom matice $\mathbf{A} \neq 0$, pokiaľ preň platia nasledujúce podmienky

1. $m(\mathbf{A}) = 0$,
2. pre všetky $f(\lambda) \in \mathbb{T}[\lambda]$ také, že $f(\mathbf{A}) = 0$ platí, že st $m(\lambda) \leq$ st $f(\lambda)$.

Poznámka. Minimálny polynóm endomorfizmu φ $m_{U,\varphi}$ môžme chápať aj ako minimálny polynóm matice $\mathbf{A}$ endomorfizmu φ, keďže $m_{U,\varphi}$ sme definovali ako normovaný polynóm najnižšieho stupňa $m_{U,\varphi} = \sum_{i=1}^n a_i x^i$ taký, že $m_{U,\varphi} u = \sum_{i=1}^n a_i \varphi^i(u) = 0$ pre všetky $u \in U$, a $\varphi^i(u) = \mathbf{A}^i u$.

Veta 2.29. *Nech $m(\lambda)$ je minimálny polynóm nenulovej matice $\mathbf{A}$ tvaru $n \times n$. Potom $m(\lambda)$ je rovný poslednému polynómu $p_n(\lambda)$ na diagonále kanonického tvaru jej charakteristickej matice $\mathbf{A} - \lambda\mathbf{E}$.*

Dôkaz. Najskôr dokážeme, že $p_n(\mathbf{A}) = 0$. Vieme, že

$$(-1)^n \det(\mathbf{A} - \lambda\mathbf{E}) = d_n^{A-\lambda E} = (-1)^n p_n(\lambda) d_{n-1}^{A-\lambda E}.$$

Označme $\mathbf{B}(\lambda)$ ako transponovanú maticu algebraických doplnkov matice $\mathbf{A} - \lambda\mathbf{E}$. Potom platí

$$(\mathbf{A} - \lambda\mathbf{E})\mathbf{B}(\lambda) = \det(\mathbf{A} - \lambda\mathbf{E})\mathbf{E}.$$

Keďže $d_{n-1}^{A-\lambda E}$ je NSD všetkých minorov matice $\mathbf{A} - \lambda\mathbf{E}$ veľkosti $n-1$, tak maticu algebraických doplnkov môžme rozpísať ako $\mathbf{B}(\lambda) = d_{n-1}^{A-\lambda E}\mathbf{C}(\lambda)$, kde NSD všetkých prvkov matice $\mathbf{C}(\lambda)$ je 1. Odtiaľ dostávame

$$\begin{aligned}(-1)^n p_n(\lambda) d_{n-1}^{A-\lambda E}\mathbf{E} &= (-1)^n \det(\mathbf{A} - \lambda\mathbf{E})\mathbf{E} = (-1)^n (\mathbf{A} - \lambda\mathbf{E})\mathbf{B}(\lambda) \\ &= (-1)^n (\mathbf{A} - \lambda\mathbf{E}) d_{n-1}^{A-\lambda E}\mathbf{C}(\lambda),\end{aligned}$$

odkiaľ plynie rovnosť $p_n(\lambda)\mathbf{E} = (\mathbf{A} - \lambda\mathbf{E})\mathbf{C}(\lambda)$, kde po dosadení $\mathbf{A}$ za λ v $p_n(\lambda)$ dostávame požadovanú rovnosť $p_n(\mathbf{A}) = 0$.
Z poslednej rovnosti plynie, že $p_n(\lambda) = q(\lambda)m(\lambda)$ pre nejaké $q(\lambda) \in \mathbb{T}[\lambda]$. Pokiaľ dokážeme, že $q(\lambda) = 1$, dôkaz bude hotový. Podľa vety 2.20 vydelíme polynóm $m(\lambda)\mathbf{E}$ polynómom $(\mathbf{A} - \lambda\mathbf{E})$ a dostaneme

$$m(\lambda)\mathbf{E} = (\mathbf{A} - \lambda\mathbf{E})\mathbf{Q}(\lambda) + \mathbf{R},$$

kde $\mathbf{R} = m(\mathbf{A}) = 0$. Odtiaľ dostávame

$$(\mathbf{A} - \lambda\mathbf{E})\mathbf{C}(\lambda) = p_n(\lambda)\mathbf{E} = q(\lambda)m(\lambda)\mathbf{E} = q(\lambda)(\mathbf{A} - \lambda\mathbf{E})\mathbf{Q}(\lambda),$$

kde po úprave vidíme, že

$$(\mathbf{A}-\lambda\mathbf{E})(\mathbf{C}(\lambda)-q(\lambda)\mathbf{Q}(\lambda))=0.$$

Vedúci koeficient matice $\mathbf{A}-\lambda\mathbf{E}$ je regulárna matica, z čoho podľa lemy 2.19 vyplýva, že súčin sa bude rovnať nule iba v prípade, že sa druhá zátvorka bude rovnať nule. Keďže NSD všetkých prvkov matice $\mathbf{C}(\lambda)$ je 1, tak zo vzťahu

$$\mathbf{C}(\lambda)=q(\lambda)\mathbf{Q}(\lambda)$$

dostávame požadovanú rovnosť $q(\lambda)=1$. □

Lema 2.30. *Nech g je charakteristický polynóm matice $\mathbf{A}$ endomorfizmu $\varphi: U\to U$ v nejakej báze α. Potom minimálny polynóm $m_{U,\varphi}$ delí g.*

Dôkaz. Dôkaz plynie z definície kanonického tvaru a predchádzajúcej vety. Charakteristický polynóm matice $\mathbf{A}$ je súčinom všetkých prvkov na diagonále kanonického tvaru matice $\mathbf{A}-\lambda\mathbf{E}$, pričom posledným prvkom je práve minimálny polynóm $m_{U,\varphi}$. □

2.4 Dôkaz Jordanovej vety

Predchádzajúce poznatky využijeme k algebraickému dôkazu Jordanovej vety. Nech U je vektorový priestor dimenzie n s bázou $\alpha=(u_1,u_2,\dots,u_n)$, na ktorom definujeme endomorfizmus $\varphi: U\to U$ s príslušnou maticou endomorfizmu $(\varphi)_{\alpha,\alpha}=\mathbf{A}$ vzhľadom k báze α. V $\mathbb{T}[x]-$module nad priestorom U existuje podľa vety 2.12 minimálny polynóm $m_{U,\varphi}$, ktorý môžme podľa vety 2.4 rozložiť na súčin ireducibilných normovaných polynómov nasledovne

$$m_{U,\varphi}=f_1^{k_1}f_2^{k_2}\dots f_r^{k_r},$$

kde k_i sú prirodzené čísla.

Lema 2.31. *Nech g je charakteristický polynóm endomorfizmu φ, ktorý má súčet algebraických násobností vlastných čísel rovný $\dim U=n$, f je ireducibilný, normovaný polynóm deliaci $m_{U,\varphi}$ a λ_i pre $i=1,2,\dots,n$ sú vlastné čísla endomorfizmu φ. Potom*

$$f=x-\lambda_i$$

pre niektoré vlastné číslo λ_i.

Dôkaz. Charakteristický polynóm napíšeme ako

$$g=(x-\lambda_1)^{l_1}(x-\lambda_2)^{l_2}\dots(x-\lambda_n)^{l_n}. \tag{2.5}$$

Vieme, že $m_{U,\varphi}|g$ a teda z predpokladu, že $f|m_{U,\varphi}$ vidíme, že $f|g$. Podľa vety 2.4 vieme, že rozklad polynómu na ireducibilné, normované polynómy je jednoznačný. Preto z (2.5) vidieť, že $f=x-\lambda_i$ pre niektoré i. □

Veta 2.32. *Majme vektorový priestor U s endomorfizmom $\varphi : U \to U$. Nech minimálny polynóm $m_{U,\varphi} = f_1^{k_1} f_2^{k_2} \dots f_r^{k_r}$, kde všetky f_i sú ireducibilné normované polynómy, pre ktoré definujeme $\mathbb{T}[x]-$podmoduly M_i nasledovne*

$$M_i = \{u \in U | f_i^{k_i} u = 0\}.$$

Potom U je direktný súčet týchto podmodulov

$$U = M_1 \oplus M_2 \oplus \dots \oplus M_r.$$

Poznámka. Pripomeňme, že koreňový podpriestor $\mathscr{R}_{\lambda_i}$ sme definovanovali v 1.18 tak, že použitím konečného počtu iterácii endomorfizmu $\varphi - \lambda_i \mathrm{id}$ na vektory z tohoto podpriestoru ich zobrazíme do 0. Všimnime si paralelu s definíciou $\mathbb{T}[x]-$podmodulov M_i, ktorých vektory sa tiež po konečnom počte násobenia polynómom f_i zobrazia do 0. Ak pripojíme poznatky z definície $\mathbb{T}[x]-$modulu 2.10 a podľa lemy 2.31 vezmeme ireducibilný normovaný polynóm $f = x - \lambda_i$ deliaci minimálny polynóm $m_{U,\varphi}$, tak dostaneme pri koeficientoch $a_1 = 1, a_0 = -\lambda_i$ vzťah

$$fu = (x - \lambda_i)u = xu - \lambda_i u = \varphi(u) - \lambda_i u = (\varphi - \lambda_i \mathrm{id})u.$$

Vidíme, že existuje prirodzené k také, že pre všetky $u \in \mathscr{R}_{\lambda_i}$ platí $f^k u = (\varphi - \lambda_i \mathrm{id})^k u = 0$ a preto môžme zobrať $\mathbb{T}[x]-$podmoduly M_i definované pomocou polynómov $(x - \lambda_i)$ takých, že $(x - \lambda_i)^{k_i} u = 0$ pre $u \in M_i$ za koreňové podpriestory definované vzťahom $(\varphi - \lambda_i \mathrm{id})^{k_i} u = 0$. Predchádzajúca veta, ktorá narába s pojmom podmodulov M_i, hovorí o rovnakom rozložení vektorového priestoru U na direktný súčet ako veta 1.18 o rozklade U na koreňové podpriestory $\mathscr{R}_{\lambda_i}$, pričom počet takýchto podpriestorov označený písmenom k v prvej kapitole sme v predchádzajúcom vyjadrení označili písmenom r. Zároveň si však všimnime, že veta 2.32 je všeobecnejšia, keďže sa neobmedzuje len na polynómy v tvare $(x - \lambda_i)^{k_i}$. Taktiež jej dôkaz je odlišný od dôkazu vety 1.18.

Dôkaz. Veta platí, pokiaľ súčet podpriestorov M_i tvorí celý priestor U a zároveň podľa lemy 1.9

$$M_i \cap \sum_{\substack{j=1 \\ i \neq j}}^{r} M_j = 0.$$

Nech vektor $u \in M_i \cap \sum M_j$, kde $j \neq i$. Potom $f_i^{k_i} u = 0$. Zároveň však aj $\overline{f}_i u = 0$, keďže vektor $u \in M_i \cap \sum M_j$ leží určite v niektorom M_j pre $j \neq i$ a polynóm $\overline{f}_i$ je podľa vety 2.9 násobkom polynómu $f_j^{k_j}$, čiže $\overline{f}_i u = \overline{f'}_i f_j^{k_j} u = 0$, kde $\overline{f'}_i$ dostaneme vydelením polynómu $\overline{f}_i$ polynómom $f_j^{k_j}$. Podľa prvého bodu vety 2.9 existujú v $\mathbb{T}[x]$-module polynómy β_i a γ_i také, že $f_i^{k_i} \beta + \overline{f}_i \gamma_i = 1$. Odtiaľ $u = \beta_i f_i^{k_i} u + \gamma_i \overline{f}_i u$, kde obi dva sčítance sú rovné 0 a teda dostávame, že $u = 0$. Preto $M_i \cap \sum M_j = 0$ pre $j \neq i$.
Podľa druhého bodu vety 2.9 existujú v $\mathbb{T}[x]$ polynómy $\alpha_1, \alpha_2, \dots, \alpha_r$ také, že

$$u = \alpha_1 \overline{f}_1 u + \alpha_2 \overline{f}_2 u + \alpha_r \overline{f}_r u. \tag{2.6}$$

Pretože $m_{U,\varphi} = f_i^{k_i} \overline{f}_i$ je minimálny polynóm, je $\overline{f}_i u \in M_i$ a teda všetky sčítance z (2.6) ležia v príslušných podpriestoroch M_i a preto ich kombinácia bude ležať v $\sum_{i=1}^{r} M_i$.

□

Veta 2.33. *Ľubovoľný podmodul M_i z vety 2.32 môžme rozložiť na direktný súčet podmodulov*

$$M_i = \langle u_1 \rangle \oplus \langle u_2 \rangle \oplus \ldots \oplus \langle u_l \rangle.$$

Poznámka. Rovnako ako sme v geometrickom dôkaze koreňové podpriestory delili ďalej na direktný súčet podpriestorov s cyklickým endomorfizmom a značili sme ich V_j, tak aj predchádzajúca veta 2.33 hovorí o takomto rozklade. Na každom $\mathbb{T}[x]-$podmodule (koreňovom podpriestore $\mathscr{R}_{\lambda_i}$) máme opäť $\mathbb{T}[x]-$podmodul určený vektorom $u \in M_i$ takým, že pre nejaké prirodzené k sa $f^k u = 0$, ale $f^{k-1} u \neq 0$, pričom všetky prvky $f^i u$, kde $0 \leq i \leq k$ očividne ležia v M_i a opakovaným násobením polynómom f_i vytvoríme cyklický reťazec, na konci ktorého sa pôvodný vektor u po k iteráciach, teda po k vynásobeniach polynómom f_i, bude rovnať nule. Podstatný rozdiel medzi vetou 2.33 o rozklade koreňového podpriestoru podľa cyklických endomorfizmov a predchádzajúcou vetou je v tom, že tento algebraický prístup rozdeľuje M_i priamo na reťazce generované práve jedným vektorom, pričom geometrický dôkaz pracoval s rozkladom podľa obrazov endomorfizmu s dimenziou nie nutne rovnou jednej. Tieto jednoznačne určené dimenzie nám neskôr pomohli dokázať jednoznačnosť JKT, čo v tomto prípade využiť nemôžme.

Dôkaz. Každý podpriestor M_i môžme vďaka vete 2.16 rozložiť na direktný súčet

$$\langle u_1 \rangle \oplus N_1.$$

Pripomeňme, že u_1 je taký vektor v M_i, že $f_i^{k_i - 1} u \neq 0$ a podmodul $N_1 \in M_i$ je maximálnym podmodulom neobsahujúcom vektor $f_i^{k_i-1} u_1$. Potom v N_1 existuje vektor u_2 taký, že pre nejaké prirodzené $k' \leq k_i$ sa $f_i^{k'} u = 0$ a zároveň $f_i^{k'-1} u \neq 0$ a k takémuto vektoru existuje v N_1 aj maximálny podmodul N_2 taký, že vektor $f_i^{k'-1} u_2$ neleží v podmodule N_2. Potom

$$N_1 = \langle u_2 \rangle \oplus N_2.$$

Postupne môžme celé M_i rozložiť na direktný súčet $\mathbb{T}[x]-$podmodulov generovaných vždy jedným prvkom

$$M_i = \langle u_1 \rangle \oplus \langle u_2 \rangle \oplus \ldots \oplus \langle u_p \rangle,$$

kde platí, že $f_i^{k_i} \langle u_j \rangle = 0$ pre $j = 1, 2, \ldots, p$. ☐

Lema 2.34. *Nech $f = x - \lambda$. Nech $u \in U$ je také, že $f^k u = 0$ a $f^{k-1} u \neq 0$ pre nejaké prirodzené k. Potom $\mathbb{T}[x]-$podmodul $\langle u \rangle$ má bázu $\{u, fu, \ldots, f^{k-1} u\}$.*

Poznámka. Zatiaľ čo v geometrickom dôkaze sme bázu podpriestoru $\mathscr{R}_{\lambda_i}$ rozloženého na direktný súčet invariantných podpriestorov s cyklickým endomorfizmom dostali priamo pri dôkaze vety 1.21 o tomto rozklade, tak vo vyššie uvedenej vete 2.33 sme určenie bázy opomenuli. Predchádzajúca lema 2.34 sa však tomuto problému venuje a vidíme, že ľubovoľný podpriestor V_j zo schémy na strane 16 s bázou určenou príslušným $j-$tym stĺpcom, čiže reťazcom zobrazení vektoru u_j endomorfizmom $\psi = \varphi - \lambda_i \mathrm{id}$, sa zhoduje s niektorým $\mathbb{T}[x]-$podmodulom $\langle u_j \rangle$ z lemy 2.33 s bázou $(u_j, fu_j, \ldots, f^{k-1} u_j)$.

Dôkaz. Pripomeňme, že aby bola množina bázou nejakého priestoru, v našom prípade $\mathbb{T}[x]-$podmodulu, musí ho generovať a byť lineárne nezávislá. Aby bola lineárne nezávislá, musia v rovnosti

$$a_1 u + a_2 f u + \ldots + a_k f^{k-1} u = 0 \tag{2.7}$$

byť všetky a_i rovné nule. Po vynásobení (2.7) polynómom f^{k-1} dostaneme

$$a_1 f^{k-1} u = 0,$$

čo platí iba ak $a_1 = 0$. Postupujeme indukciou podľa $i = 1, 2, \ldots, k-1$, kde predpokladáme, že $a_1 = a_2 = \ldots = a_i = 0$ a po vynásobení (2.7) polynómom f^{k-i-1} dostávame

$$a_{i+1} f^{k-1} u = 0,$$

odkiaľ nutne $a_{i+1} = 0$. Postupne dokážeme, že $a_i = 0$ pre všetky $i = 1, 2, \ldots, k$ a teda naša množina je lineárne nezávislá.
Ak množina vektorov generuje $\mathbb{T}[x]-$podmodul $\langle u \rangle$, tak to znamená, že ľubovoľný nenulový prvok $gu \in \langle u \rangle$, kde $g \in \mathbb{T}[x]$, môžme napísať ako kombináciu prvkov našej uvažovanej množiny. Polynóm g môžme rozpísať ako

$$g = \sum_{j=0}^{n} a_j x^j = \sum_{j=0}^{n} a_j \big((x-\lambda)+\lambda\big)^j = \sum_{j=0}^{n} b_j (x-\lambda)^j,$$

kde využijeme vzťah z lemy 2.31 $f = x - \lambda$ a dostaneme nalsedujúci tvar polynómu

$$g = \sum_{j=0}^{n} b_j f^j.$$

Po aplikácii na vektor u máme

$$gu = \sum_{j=0}^{n} b_j f^j u,$$

kde pre $j \geq k$ je $f^j u = 0$ a preto dostávame gu v požadovanom tvare

$$gu = \sum_{j=0}^{k-1} b_j f^j u.$$

□

Dôkaz Jordanovej vety pre endomorfizmy. Nech U je vektorvý priestor s dimenziou rovnou n a s endomorfizmom $\varphi : U \to U$, ktorého súčet algebraických násobnosti vlastných čísel je rovný n. Vektorový priestor U môžme podľa vety 2.32 rozložiť na direktný súčet $\mathbb{T}[x]-$podmodulov M_i určenými ireducibilnými normovanými polynómami $f_i = x - \lambda_i$ deliacimi minimálny polynóm $m_{U,\varphi}$, čiže

$$U = M_1 \oplus M_2 \oplus \ldots \oplus M_r.$$

Podmoduly M_i môžme zas podľa vety 2.33 rozložiť na direktný súčet $\mathbb{T}[x]-$podmodulov generovaných jedným prvkom $\langle u \rangle$

$$M_i = \langle u_1 \rangle \oplus \langle u_2 \rangle \oplus \ldots \oplus \langle u_p \rangle.$$

Podľa lemy 2.34 je endomorfizmus $\varphi - \lambda_i\mathrm{id}$ cyklický na každom $\langle u_j\rangle$. Nájdeme bázu v každom takomto $\mathbb{T}[x]-$podmodule $\langle u_j\rangle$, tieto bázy zjednotíme a vďaka direktnému súčtu dostaneme bázu celého M_i. Rovnako po zjednotení báz všetkých M_i dostaneme bázu celého $\mathbb{T}[x]-$modulu. Matica endomorfizmu bude mať vďaka invariantnosti M_i a $\mathbb{T}[x]-$podmodulov v nich podľa vety 1.14 blokovo diagonálny tvar. Stačí nám nájsť bázy jednotlivých $\mathbb{T}[x]$-podmodulov $\langle u_j\rangle$, pre ktoré bude mať matica endomorfizmu $\varphi|_{\langle u\rangle}$ tvar Jordanovej bunky. Vďaka vzťahu $f_i = x - \lambda_i$ ukážeme, že báza

$$\widetilde{\alpha} = (u, f_i u, \dots, f_i^{k-1}u)$$

z lemy 2.34 spĺňa požadovanú vlastnosť:

$$\begin{aligned}
\varphi(u) = &\quad xu &&= \lambda_i u + f_i u\\
\varphi(f_i u) = &\quad x f_i u &&= \lambda_i f_i u + f_i^2 u\\
\varphi(f_i^2 u) = &\quad x f_i^2 u &&= \lambda_i f_i^2 u + f_i^3 u\\
\\
\varphi(f_i^{k-2} u) = &\quad x f_i^{k-2} u &&= \lambda_i f_i^{k-2} u + f_i^{k-1} u\\
\varphi(f_i^{k-1} u) = &\quad x f_i^{k-1} u &&= \lambda_i f_i^{k-1} u + f_i^{k} u = \lambda_i f_i^{k-1} u.
\end{aligned}$$

Keď zostavíme pomocou tejto schémy maticu endomorfizmu $\varphi|_{\langle u\rangle}$ v báze $\widetilde{\alpha}$, dostávame Jordanovu bunku s príslušnými vlastnými číslami λ_i na diagonále a jednotkami nad hlavnou diagonálou.
K dôkazu jednoznačnosti Jordanovho kanonického tvaru využijeme kanonický tvar matice endomorfizmu. Dve rôzne matice endomorfizmu φ sú podobné, čo znamená, že matica v Jordnaovom kanonickom tvare, ktorú nazveme $\mathbf{J}$, bude podobná s ľubovoľnou maticou endomorfizmu v nejakej inej báze. Podľa vety 2.24 sú ich charakteristické matice $\mathbf{A} - \lambda\mathbf{E}$ a $\mathbf{J} - \lambda\mathbf{E}$ ekvivalentné, čo zas podľa vety 2.27 znamená, že majú rovnaký kanonický tvar $\mathbf{K}(\lambda)$. Stačí nám nájsť algoritmus, ktorý preukáže jednoznačnosť medzi kanonickým tvarom matice $\mathbf{A} - \lambda\mathbf{E}$, a teda aj matice $\mathbf{J} - \lambda\mathbf{E}$, a Jordanovym kanonickým tvarom matice endomorfizmu – maticou $\mathbf{J}$, ktorá bude podobná všetkým maticiam endomorfizmu φ bez ohľadu na výber bázy. Tento algoritmus si ukážeme na príkladoch jednotlivých možných situácii.

1. Určíme kanonický tvar $\lambda-$matice $\mathbf{J} - \lambda\mathbf{E}$, kde $\mathbf{J}$ je Jordanova bunka veľkosti k s vlastným číslom λ_1.

$$\mathbf{J} = \begin{pmatrix}
\lambda_1 & 1 & 0 & & \dots & 0\\
0 & \lambda_1 & 1 & & \dots & 0\\
0 & 0 & \lambda_1 & & \dots & 0\\
\vdots & & & \ddots & & \vdots\\
0 & & \dots & & \lambda_1 & 1\\
0 & & \dots & & 0 & \lambda_1
\end{pmatrix}$$

Najmenší nenulový spoločný deliteľ d_1^J je určite rovný 1. Rovnako všetky nenulové minory veľkosti 2 budú mať NSD=1, čo sú minory submatíc nad hlavnou diagonálou

$\left(\begin{smallmatrix} 1 & 0 \\ \lambda_1-\lambda & 1 \end{smallmatrix}\right)$. Týmto spôsobom zistíme, že najväčší spoločný deliteľ minorov rôznych veľkostí bude rovný jednej až po d_{k-1}^J. V prípade d_k^J ide o determinant našej matice, ktorý po úprave na normovaný tvar je rovný $(\lambda-\lambda_1)^k$. Kanonický tvar Jordanovej bunky veľkosti k bude mať preto tvar $\mathbf{K}(\lambda) = \operatorname{diag}\big(1,1,\ldots,1,(\lambda-\lambda_1)^k\big)$.

2. Určíme kanonický tvar $\lambda-$matice $\mathbf{J}-\lambda\mathbf{E}$ pozostávajúcej z dvoch Jordanovych buniek veľkosti k a m, kde $k<m$, s vlastným číslom λ_1. Pre jednoduchosť zvoľme napríklad $k=3$ a $m=4$.

$$\mathbf{J} = \left(\begin{array}{ccc|cccc} \lambda_1 & 1 & 0 & & & & \\ 0 & \lambda_1 & 1 & & 0 & & \\ 0 & 0 & \lambda_1 & & & & \\ \hline & & & \lambda_1 & 1 & 0 & 0 \\ & & & 0 & \lambda_1 & 1 & 0 \\ & 0 & & 0 & 0 & \lambda_1 & 1 \\ & & & 0 & 0 & 0 & \lambda_1 \end{array}\right)$$

Nad hlavnou diagonálou máme 5 jednotiek, z čoho podľa predchádzajúceho príkladu vidíme, že $d_i^J = 1$ pre $i = 1,2,\ldots,5$. Pre $i=6$ bude NSD príslušných minorov $(\lambda-\lambda_1)^3$ reprezentujúci maticu po vyškrtnutí 4. stĺpca a posledného riadku. Pre $i=7$ ide opäť o normovaný determinant matice rovný $(\lambda-\lambda_1)^7$. V dôkaze vety 2.27 sme dokázali vzťah medzi polynómami z kanonického tvaru a najväčšími spoločnými deliteľmi

$$p_k = \frac{d_k^A}{d_{k-1}^A}.$$

Vďaka tomu určíme kanonický tvar $\mathbf{K}(\lambda) = \operatorname{diag}\big(1,1,\ldots,1,(\lambda-\lambda_1)^3,(\lambda-\lambda_1)^4\big)$.

3. Určíme kanonický tvar $\lambda-$matice $\mathbf{J}-\lambda\mathbf{E}$ pozostávajúcej z dvoch Jordanovych buniek veľkosti k a m, kde $k<m$, s dvoma rôznymi vlastnými číslami λ_1 a λ_2. Pre jednoduchosť zvoľme napríklad $k=3$ a $m=4$.

$$\mathbf{J} = \left(\begin{array}{ccc|cccc} \lambda_1 & 1 & 0 & & & & \\ 0 & \lambda_1 & 1 & & 0 & & \\ 0 & 0 & \lambda_1 & & & & \\ \hline & & & \lambda_2 & 1 & 0 & 0 \\ & & & 0 & \lambda_2 & 1 & 0 \\ & 0 & & 0 & 0 & \lambda_2 & 1 \\ & & & 0 & 0 & 0 & \lambda_2 \end{array}\right)$$

Podobne ako v predchádzajúcom bode bude $d_i^J = 1$ pre $i = 1,2,\ldots,5$. Pre $i=6$ neexistuje spoločný deliteľ okrem 1, keďže nenulové minory veľkosti 6 sú aj $(\lambda_1-\lambda)^3$ po vyškrtnutí 4. stĺpca a posledného riadku, aj $(\lambda_2-\lambda)^4$ po vyškrtnutí prvého stĺpca a 3. riadku. d_7^J je normovaný determinant matice $\mathbf{J}-\lambda\mathbf{E}$ rovný $(\lambda-\lambda_1)^3(\lambda-\lambda_2)^4$. Preto kanonický tvar bude $\mathbf{K}(\lambda) = \operatorname{diag}\big(1,1,\ldots,1,(\lambda-\lambda_1)^3(\lambda-\lambda_2)^4\big)$.

Majme teda kanonický tvar matice $\mathbf{A} - \lambda\mathbf{E}$

$$\mathbf{K}(\lambda) = \begin{pmatrix} p_1(\lambda) & 0 & \dots & 0 \\ 0 & p_2(\lambda) & & 0 \\ \vdots & & \ddots & \vdots \\ 0 & \dots & & p_n(\lambda) \end{pmatrix},$$

Polynómy p_i rozpíšeme nasledovne

$$\begin{aligned} p_1 &= (\lambda-\lambda_1)^{k_1}(\lambda-\lambda_2)^{l_1}\dots \\ p_2 &= (\lambda-\lambda_1)^{k_2}(\lambda-\lambda_2)^{l_2}\dots \\ &\vdots \\ p_n &= (\lambda-\lambda_1)^{k_n}(\lambda-\lambda_2)^{l_n}\dots . \end{aligned}$$

Keďže p_i delí p_{i+1}, tak určite platí

$$k_1 \le k_2 \le \dots \le k_n,$$

$$l_1 \le l_2 \le \dots \le l_n,$$

$$\vdots$$

pre všetky vlastné čísla λ_j. Platí, že Jordanove bunky príslušné vlastnému číslu λ_1 majú rozmery $k_1, k_2, \dots, k_n$, Jordanove bunky pre vlastné číslo λ_2 majú rozmery $l_1, l_2, \dots, l_n$ a takýmto spôsobom nájdeme veľkosti a počty všetkých Jordanových buniek v JKT. □

2.5 Algoritmus hľadania Jordanovho kanonického tvaru

Majme ľubovoľnú maticu $\mathbf{A}$ endomorfizmu φ. Vieme, že jej charakteristická matica $\mathbf{A} - \lambda\mathbf{E}$ je ekvivalentá s maticou $\mathbf{J} - \lambda\mathbf{E}$, čo znamená, že majú rovnaký kanonický tvar. Tieto poznatky využijeme pri hľadaní JKT a matice prechodu medzi $\mathbf{A}$ a $\mathbf{J}$. V prvom rade prevedieme maticu $\mathbf{A} - \lambda\mathbf{E}$ riadkovými a stĺpcovými elementárnymi úpravami na kanonický tvar

$$\begin{array}{c|c} \mathbf{A}-\lambda\mathbf{E} & \mathbf{E} \\ \hline \mathbf{E} & \end{array} \sim \dots \sim \begin{array}{c|c} \mathbf{K}(\lambda) & \widetilde{\mathbf{P}}(\lambda) \\ \hline \widetilde{\mathbf{Q}}(\lambda) & \end{array},$$

pričom platí, že $\mathbf{K}(\lambda) = \widetilde{\mathbf{P}}(\lambda)(\mathbf{A}-\lambda\mathbf{E})\widetilde{\mathbf{Q}}(\lambda)$. Z kanonického tvaru matice vieme jednoznačne určiť maticu v Jordanovom kanonickom tvare a teda aj jej charakteristickú maticu. Tú opäť riadkovými a stĺpcovými elementárnymi operáciami prevedieme na kanonický tvar

$$\begin{array}{c|c} \mathbf{J}-\lambda\mathbf{E} & \mathbf{E} \\ \hline \mathbf{E} & \end{array} \sim \dots \sim \begin{array}{c|c} \mathbf{K}(\lambda) & \overline{\mathbf{P}}(\lambda) \\ \hline \overline{\mathbf{Q}}(\lambda) & \end{array},$$

pričom platí, že $\mathbf{K}(\lambda) = \overline{\mathbf{P}}(\lambda)(\mathbf{J}-\lambda\mathbf{E})\overline{\mathbf{Q}}(\lambda)$.
Z rovnosti $\mathbf{K}(\lambda)$ dostávame po úprave rovnicu

$$\mathbf{J}-\lambda\mathbf{E} = \overline{\mathbf{P}}^{-1}(\lambda)\widetilde{\mathbf{P}}(\lambda)(\mathbf{A}-\lambda\mathbf{E})\widetilde{\mathbf{Q}}(\lambda)\overline{\mathbf{Q}}^{-1}(\lambda).$$

Výraz $\overline{\mathbf{P}}^{-1}(\lambda)\widetilde{\mathbf{P}}(\lambda)$ pre jednoduchosť nahradíme výrazom $\mathbf{P}(\lambda)$. Rovnako položíme $\mathbf{Q}(\lambda) = \widetilde{\mathbf{Q}}(\lambda)\overline{\mathbf{Q}}^{-1}(\lambda)$. Dostaneme rovnosť

$$\mathbf{J} - \lambda\mathbf{E} = \mathbf{P}(\lambda)(\mathbf{A} - \lambda\mathbf{E})\mathbf{Q}(\lambda).$$

Postupujeme rovnako ako v dôkaze kritéria ekvivalencie 2.24. Vďaka vete 2.20 rozložíme $\mathbf{P}$ a $\mathbf{Q}$:

$$\mathbf{P}(\lambda) = (\mathbf{J} - \lambda\mathbf{E})\mathbf{P}_1 + \mathbf{P}_0$$
$$\mathbf{Q}(\lambda) = \mathbf{Q}_1(\mathbf{J} - \lambda\mathbf{E}) + \mathbf{Q}_0$$

a postupnými úpravami s využitím predchádzajúcich troch rovníc, rovnako ako v spomenutom dôkaze, dostaneme vzťah

$$\mathbf{J} - \lambda\mathbf{E} = \mathbf{P}_0(\mathbf{A} - \lambda\mathbf{E})\mathbf{Q}_0,$$

odkiaľ po porovnaní koeficientov pri λ^1 a λ^0 dostaneme

$$\mathbf{J} = \mathbf{P}_0\mathbf{A}\mathbf{P}_0^{-1}.$$

Všimneme si, že $\mathbf{P}_0$ dostaneme dosadením matice $\mathbf{J}$ do polynómu $\mathbf{P}(\lambda)$ zľava, čo dáva jednoduchý návod na vypočítanie $\mathbf{P}_0$.

Príklad 2.35. Ukážeme si na príklade ako nájdeme Jordanov kanonický tvar $\mathbf{J}$ a maticu prechodu $\mathbf{P}$. Majme maticu

$$\mathbf{A} = \begin{pmatrix} 3 & 2 & -3 \\ 4 & 10 & -12 \\ 3 & 6 & -1 \end{pmatrix}.$$

Riadkovými a stĺpcovými elementárnymi operáciami ju upravujeme na kanonický tvar, pričom sa nám z jednotkových matíc formujú aj matice $\widetilde{\mathbf{P}}(\lambda)$ a $\widetilde{\mathbf{Q}}(\lambda)$.

$$\left(\begin{array}{ccc|ccc} 3-\lambda & 2 & -3 & 1 & 0 & 0 \\ 4 & 10-\lambda & -12 & 0 & 1 & 0 \\ 3 & 6 & -7-\lambda & 0 & 0 & 1 \\ \hline 1 & 0 & 0 & & & \\ 0 & 1 & 0 & & & \\ 0 & 0 & 1 & & & \end{array}\right) \sim \left(\begin{array}{ccc|ccc} 4 & 10-\lambda & 12 & 0 & 1 & 0 \\ 3 & 6 & -7-\lambda & 0 & 0 & 1 \\ 3-\lambda & 2 & -3 & 1 & 0 & 0 \\ \hline 1 & 0 & 0 & & & \\ 0 & 1 & 0 & & & \\ 0 & 0 & 1 & & & \end{array}\right) \sim$$

$$\sim \left(\begin{array}{ccc|ccc} 1 & 4-\lambda & -5+\lambda & 0 & 1 & -1 \\ 3 & 6 & -7-\lambda & 0 & 0 & 1 \\ 3-\lambda & 2 & -3 & 1 & 0 & 0 \\ \hline 1 & 0 & 0 & & & \\ 0 & 1 & 0 & & & \\ 0 & 0 & 1 & & & \end{array}\right) \sim$$

$$\sim \left(\begin{array}{ccc|ccc} 1 & 4-\lambda & -5+\lambda & 0 & 1 & -1 \\ 0 & -3(2-\lambda) & 4(2-\lambda) & 0 & -3 & 4 \\ 0 & (2-\lambda)(\lambda-5) & (\lambda-2)(\lambda-6) & 1 & \lambda-3 & 3-\lambda \\ \hline 1 & 0 & 0 & & & \\ 0 & 1 & 0 & & & \\ 0 & 0 & 1 & & & \end{array}\right) \sim$$

$$\sim \left(\begin{array}{ccc|ccc} 1 & 0 & 0 & 0 & 1 & -1 \\ 0 & -3(2-\lambda) & 4(2-\lambda) & 0 & -3 & 4 \\ 0 & (2-\lambda)(\lambda-5) & (\lambda-2)(\lambda-6) & 1 & \lambda-3 & 3-\lambda \\ \hline 1 & \lambda-4 & 5-\lambda & & & \\ 0 & 1 & 0 & & & \\ 0 & 0 & 1 & & & \end{array}\right) \sim$$

$$\sim \left(\begin{array}{ccc|ccc} 1 & 0 & 0 & 0 & 1 & -1 \\ 0 & (2-\lambda) & 4(2-\lambda) & 0 & -3 & 4 \\ 0 & (2-\lambda) & (\lambda-2)(\lambda-6) & 1 & \lambda-3 & 3-\lambda \\ \hline 1 & 1 & 5-\lambda & & & \\ 0 & 1 & 0 & & & \\ 0 & 1 & 1 & & & \end{array}\right) \sim$$

$$\sim \left(\begin{array}{ccc|ccc} 1 & 0 & 0 & 0 & 1 & -1 \\ 0 & \lambda-2 & 0 & 0 & -3 & 4 \\ 0 & 0 & (\lambda-2)^2 & 1 & \lambda & -1-\lambda \\ \hline 1 & 1 & 1-\lambda & & & \\ 0 & 1 & -4 & & & \\ 0 & 1 & -3 & & & \end{array}\right)$$

Kanonická matica je tvaru

$$\mathbf{K}(\lambda) = \begin{pmatrix} 1 & 0 & 0 \\ 0 & \lambda-2 & 0 \\ 0 & 0 & (\lambda-2)^2 \end{pmatrix} = \begin{pmatrix} 0 & 1 & -1 \\ & -3 & -4 \\ 1 & \lambda & -1-\lambda \end{pmatrix} (\mathbf{A}-\lambda\mathbf{E}) \begin{pmatrix} 1 & 1 & 1-\lambda \\ 0 & 1 & -4 \\ 0 & 1 & -3 \end{pmatrix}$$

$$= \widetilde{\mathbf{P}}(\lambda)(\mathbf{A}-\lambda\mathbf{E})\widetilde{\mathbf{Q}}(\lambda).$$

Z kanonickej matice jednoducho dostaneme Jordanov kanonický tvar, keďže vidíme, že má dve Jordanove bunky, obe s vlastným číslom $\lambda = 2$, jednu veľkosti 1 a jednu veľkosti 2.

$$\mathbf{J} = \begin{pmatrix} 2 & 0 & 0 \\ 0 & 2 & 1 \\ 0 & 0 & 2 \end{pmatrix}.$$

Teraz rovnakým spôsobom z matice $\mathbf{J}-\lambda\mathbf{E}$ vyjadríme kanonický tvar, pričom nájdeme $\overline{\mathbf{P}}(\lambda)$ a $\overline{\mathbf{Q}}(\lambda)$.

$$\left(\begin{array}{ccc|ccc} 2-\lambda & 0 & 0 & 1 & 0 & 0 \\ 0 & 2-\lambda & 1 & 0 & 1 & 0 \\ 0 & 0 & 2-\lambda & 0 & 0 & 1 \\ \hline 1 & 0 & 0 & & & \\ 0 & 1 & 0 & & & \\ 0 & 0 & 1 & & & \end{array}\right) \sim \left(\begin{array}{ccc|ccc} 0 & 0 & 2-\lambda & 1 & 0 & 0 \\ 1 & 2-\lambda & 0 & 0 & 1 & 0 \\ 2-\lambda & 0 & 0 & 0 & 0 & 1 \\ \hline 0 & 0 & 1 & & & \\ 0 & 1 & 0 & & & \\ 1 & 0 & 0 & & & \end{array}\right) \sim$$

$$\sim \left(\begin{array}{ccc|ccc} 1 & 2-\lambda & 0 & 0 & 1 & 0 \\ 0 & 0 & 2-\lambda & 1 & 0 & 0 \\ 2-\lambda & 0 & 0 & 0 & 0 & 1 \\ \hline 0 & 0 & 1 & & & \\ 0 & 1 & 0 & & & \\ 1 & 0 & 0 & & & \end{array}\right) \sim \left(\begin{array}{ccc|ccc} 1 & 2-\lambda & 0 & 0 & 1 & 0 \\ 0 & 0 & 2-\lambda & 1 & 0 & 0 \\ 0 & -(2-\lambda)^2 & 0 & 0 & \lambda-2 & 1 \\ \hline 0 & 0 & 1 & & & \\ 0 & 1 & 0 & & & \\ 1 & 0 & 0 & & & \end{array}\right) \sim$$

$$\sim \left(\begin{array}{ccc|ccc} 1 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 2-\lambda & 1 & 0 & 0 \\ 0 & -(2-\lambda)^2 & 0 & 0 & \lambda-2 & 1 \\ \hline 0 & 0 & 1 & & & \\ 0 & 1 & 0 & & & \\ 1 & \lambda-2 & 0 & & & \end{array}\right) \sim \left(\begin{array}{ccc|ccc} 1 & 0 & 0 & 0 & 1 & 0 \\ 0 & \lambda-2 & 0 & 1 & 0 & 0 \\ 0 & 0 & (\lambda-2)^2 & 0 & \lambda-2 & 1 \\ \hline 0 & -1 & 0 & & & \\ 0 & 0 & -1 & & & \\ 1 & 0 & 2-\lambda & & & \end{array}\right)$$

Kanonický tvar matice $\mathbf{J}-\lambda\mathbf{E}$ je rovnaký ako u $\mathbf{A}-\lambda\mathbf{E}$. Vyrátali sme matice prechodu $\overline{\mathbf{P}}$ a $\overline{\mathbf{Q}}$.

$$\mathbf{K}(\lambda) = \begin{pmatrix} 1 & 0 & 0 \\ 0 & \lambda-2 & 0 \\ 0 & 0 & (\lambda-2)^2 \end{pmatrix} = \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & \lambda-2 & 1 \end{pmatrix} (\mathbf{J}-\lambda\mathbf{E}) \begin{pmatrix} 0 & -1 & 0 \\ 0 & 0 & -1 \\ 1 & 0 & 2-\lambda \end{pmatrix}$$

$$= \overline{\mathbf{P}}(\lambda)(\mathbf{J}-\lambda\mathbf{E})\overline{\mathbf{Q}}(\lambda).$$

Z oboch rovností pre $\mathbf{K}(\lambda)$ dostávame vzťah

$$\mathbf{J}-\lambda\mathbf{E} = \overline{\mathbf{P}}^{-1}(\lambda)\widetilde{\mathbf{P}}(\lambda)(\mathbf{A}-\lambda\mathbf{E})\widetilde{\mathbf{Q}}(\lambda)\overline{\mathbf{Q}}^{-1}(\lambda) = \mathbf{P}(\lambda)(\mathbf{A}-\lambda\mathbf{E})\mathbf{Q}(\lambda),$$

čiže dopočítame $\mathbf{P}(\lambda)$, rozpíšeme ho do tvaru polynómu s maticami ako koeficientami a dosadíme maticu $\mathbf{J}$ do tohto polynómu za λ zľava, čím dostaneme maticu $\mathbf{P}_0$ takú, že

$$\mathbf{J} = \mathbf{P}_0\mathbf{A}\mathbf{P}_0^{-1}.$$

$$\mathbf{P}(\lambda) = \overline{\mathbf{P}}^{-1}(\lambda)\widetilde{\mathbf{P}}(\lambda) = \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 2-\lambda & 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 0 & 1 & -1 \\ 0 & -3 & 4 \\ 1 & \lambda & -1-\lambda \end{pmatrix} = \begin{pmatrix} 0 & -3 & 4 \\ 0 & 1 & -1 \\ 1 & 2 & -3 \end{pmatrix}.$$

Vidíme, že je to $\lambda-$matica so stupňom rovným 0, ale všeobecne si ukážeme, ako by sme postupovali, keby nám v matici **P** ostali aj nejaké λ a teda by mala stupeň rovný 1. Vyjadríme

$$\mathbf{P}(\lambda) = \lambda \cdot \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix} + \begin{pmatrix} 0 & -3 & 4 \\ 0 & 1 & -1 \\ 1 & 2 & -3 \end{pmatrix}$$

a po dosadení **J** za λ dostaneme

$$\mathbf{P}_0 = \mathbf{L}_{\mathbf{P}}(\mathbf{J}) = \begin{pmatrix} 2 & 0 & 0 \\ 0 & 2 & 1 \\ 0 & 0 & 2 \end{pmatrix} \cdot \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix} + \begin{pmatrix} 0 & -3 & 4 \\ 0 & 1 & -1 \\ 1 & 2 & -3 \end{pmatrix} = \begin{pmatrix} 0 & -3 & 4 \\ 0 & 1 & -1 \\ 1 & 2 & -3 \end{pmatrix}$$

$$\mathbf{P}_0^{-1} = \begin{pmatrix} 1 & 1 & 1 \\ 1 & 4 & 0 \\ 1 & 3 & 0 \end{pmatrix}.$$

Zoznam použitej literatúry

[1] BICAN, Ladislav. Lineární algebra a geometrie. Vyd. 2. Praha: Academia, 2009, 303 s. ISBN 978-80-200-1707-9.

[2] ČADEK, M.: Lineární algebra a geometrie III. www.math.muni.cz/~cadek, [cit. 12. apríl 2015; 17:43h SEČ]. Dostupné na webovskej stránke: https://www.math.muni.cz/~cadek/la3/SKRIPTA.pdf

[3] ROSICKÝ, Jiří. Algebra. Vyd. 4., přeprac. Brno: Masarykova univerzita, 2002. ISBN 978-80-210-2964-4.

[4] SLOVÁK, Jan.: Lineární algebra. www.math.muni.cz/~slovak, 1997/1998, [cit. 12. apríl 2015; 17:36h SEČ]. Dostupné na webovskej stránke: https://www.math.muni.cz/~slovak/Vyuka/la.pdf

[5] VOPĚNKA, Petr. Úvod do klasické teorie množin. 1. vyd. Plzeň: Vydavatelství Západočeské univerzity v Plzni, 2011, 205 s. ISBN 978-80-7043-986-9.

[6] ZLATOŠ, Pavol. Lineárna algebra a geometria: cesta z troch rozmerov s presahmi do príbuzných odborov. 1. vyd. Bratislava: Marenčin PT, 2011, 741 s. ISBN 978-80-8114-111-9.